UNIVERSIDADE DE LISBOA

FACULDADE DE CIÊNCIAS

DEPARTAMENTO DE INFORMÁTICA

SUPORTE À DECISÃO PARA AVALIAÇÃO DE SOLUÇÕES BYOD

MESTRADO EM SEGURANÇA INFORMÁTICA

Ana Paula Joaquim Gonçalves

Dissertação orientada por:
Profª. Doutora Ana Luísa do Carmo Correia Respício

2017

Agradecimentos

Agradeço a todos os professores do mestrado de segurança informática da Faculdade de Ciências de Lisboa e, em especial à Professora Ana Respício pelo apoio prestado, pela orientação na concretização deste trabalho e, pela sua disponibilidade, ajuda e contributo para o sucesso deste projeto.

Agradeço ao Engenheiro José Alegria, CSO da Portugal Telecom, pelo auxílio fundamental que me prestou e pelas sugestões de grande valor.

Agradeço também a todos os meus amigos e colegas pela constante motivação e incentivos que direta ou indiretamente me ajudaram a concretizar mais um objetivo.

Por último agradeço à minha família pelo constante apoio não só nos momentos bons, mas principalmente nos momentos menos bons e, sobretudo pelas palavras de apoio e motivação em alturas cruciais.

Resumo

Estamos cada vez mais dependentes das tecnologias de informação e dos sistemas tecnológicos. Até mesmo para executar as tarefas mais simples (como efetuar pagamentos, verificar os horários dos transportes, agendar reuniões ou verificar o email), recorremos à tecnologia. Esta dependência coloca-nos vulneráveis a questões relacionados com a confidencialidade, a integridade e disponibilidade da informação.

O fenómeno BYOD (*Bring Your Own Device*) apesar de poder ser interpretado pela maioria das organizações como conduzindo a um aumento da produtividade, dada a disponibilidade do colaborador através da utilização de diferentes dispositivos móveis, sejam eles *smartphones*, *pda's*, *laptop's* ou *tablet's*, pessoais ou da organização, apresenta riscos associados à segurança informática.

Este trabalho propõe um modelo de suporte à decisão para avaliação de soluções BYOD, sendo composto por modelos que suportam: a análise dos requisitos legais obrigatórios; a avaliação dos ativos críticos; a análise de cenários de ameaças e riscos inerentes; a análise dos possíveis controlos de segurança e/ou medidas de mitigação; a análise custo-benefício e as diretrizes para o estabelecimento de uma Política de Segurança BYOD.

Palavras-chave: BYOD, segurança, risco, avaliação de risco, dispositivos móveis

Abstract

We are increasingly dependent on information technology and system technology. Even to perform simple tasks (such as make payments, check schedules of transport, schedule meetings or send an e-mail), we turn to technology. This dependence puts us vulnerable to issues relating to the confidentiality, integrity and availability of information.

The BYOD (Bring Your Device Own) phenomenon although can be interpreted by most organizations as leading to increased productivity, given the availability of the employees used different mobile devices, like Smartphone's, PDA's, laptop's or tablet's, personal or corporate, also brings risks related to computer security.

This paper proposes a decision support model for the evaluation of BYOD solutions, which consists of models that support: the analysis of mandatory legal requirements; the assessment of critical assets; the analysis of threat scenarios and inherent risks; the analysis of possible safety controls and / or mitigation measures; the cost-benefit analysis and the guidelines for the establishment of a BYOD Security Policy.

Keywords: BYOD, security, risk, risk assessment, mobile devices

Conteúdo

Índice de Figuras

Índice de Tabelas

Lista de Abreviaturas e Siglas

BCR	Benefit-to-Cost Ratio
BIA	Business Impact Analysis
BYOD	Bring Your Own Device
CAPEX	Capital Expenditure
CBA	Cost-Benefit Analysis
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
COBIT	Control Objectives for Information and Related Technology
COPE	Corporate Owned, Personally Enabled
CSO	Chief Security Officer
DoD	U.S. Department of Defense
EMM	Enterprise Mobility Management
ENISA	European Network and Information Security Agency (ENISA)
ERM	Enterprise Risk Management
EVA	Endpoint Visibility, Access, and Security
F.B.I.	Federal Bureau of Investigation
FAIR	Factor Analysis of Information Risk
HIPAA	Health Insurance Portability and Accountability Act
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IRR	Internal Rate of Return
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library

MAR	Modelo para Avaliação dos Riscos
MCBA	Modelo de Análise Custo-Benefício
MCPSB	Modelo *Checklist* da Política de Segurança BYOD
MDM	Mobile Device Management
MPICT	Modelo de Posicionamento ICT
MRLO	Modelo de análise dos Requisitos Legais Obrigatórios
NIST	National Institute of Standards and Technology
NPV	Net Present Value
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OPEX	Operational Expenditure
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PMBOK	Project Management Body of Knowledge
PRINCE2	Project in Controlled Environments
ROI	Return on Investment
SaaS	Software as a Service
SEI	Software Engineering Institute
SGSI	Sistemas de Gestão de Segurança da Informação
SI	Sistemas de Informação
SIR	Savings to Investment Ratio
SMEs	Small and Medium-sized Enterprises
TA	Taxa de atualização
TEM	Telecom Expense Management
TIR	Taxa Interna de Rendibilidade
TOGAF	The Open Group Architecture Framework
UML	Unified Modeling Language
VAL	Valor Atual Líquido
VaR	Value at Risk
VPL	Valor Presente Líquido
VPN	Virtual Private Network
Wi-FI	Wireless Local Area Network

Capítulo 1

Introdução

BYOD (abreviatura de "*Bring Your Own Device*") pode ser definido como uma solução ou uma estratégia alternativa em que os colaboradores, parceiros de negócio e utilizadores em geral recorrem aos dispositivos pessoais para aceder a aplicações, a redes ou a dados corporativos. Esta solução consiste na utilização dos dispositivos móveis pessoais no ambiente de trabalho ou fora dele, no acesso a recursos exclusivos da empresa, como o correio eletrónico, aplicações corporativas ou a base de dados.

A generalização do uso de dispositivos móveis: *smartphones*, *pda's*, *tablet's* veio revolucionar a nossa postura pessoal e profissional. A possibilidade de estarmos ligados diariamente, a facilidade do acesso à informação, a existência de uma variedade de aplicações móveis que permitem igualmente o acesso a dados corporativos implicam novas oportunidades mas também novos desafios para os profissionais de *Information and Communications Technology* (ICT), *Chief Information Officer* (CIO) e para os responsáveis pela segurança da informação (*Chief Security Officer* ou CSO). É imprescindível implementar soluções de mobilidade seguras, fáceis de gerir e manter o controlo sobre a segurança dos dados das empresas. As organizações devem definir uma política corporativa e soluções BYOD eficazes com regras e procedimentos de atuação na utilização dos dispositivos móveis, considerando a segurança e o nível de risco.

Tal como qualquer outra tecnologia ICT, os dispositivos móveis necessitam de respeitar as principais propriedades de segurança (Mamede, 2006):

A confidencialidade que consiste em garantir que o acesso da informação é efetuado somente pelas entidades legítimas, ou seja, pelas entidades autorizadas pelo proprietário da informação, com o objetivo de prevenir acessos não autorizados.

A integridade que objetiva garantir que a informação manipulada mantém as características originais estabelecidas pelo proprietário da informação, ou seja, garantia de proteção contra a perda ou corrupção dos dados.

A disponibilidade que visa garantir que a informação está disponível para uso legítimo, isto é, para aqueles cujo acesso foi autorizado pelo proprietário da informação.

Para atingir estes objetivos, os dispositivos móveis devem estar protegidos contra uma diversidade de ameaças. Para esses dispositivos, podem ser consideradas as recomendações gerais de segurança em ICT, no entanto, os dispositivos móveis e, tendo em conta a sua natureza, estão mais expostos a ameaças do que os dispositivos habituais (exemplo *desktops* e *laptops* geralmente usados dentro das instalações e protegidos pela infraestrutura da organização). Sendo assim, os dispositivos móveis requerem proteções adicionais e um trabalho prévio de análise custo-benefício adequado à realidade e aos objetivos das organizações.

1.1 Motivação

BYOD está a tornar-se uma realidade e uma prática comum nas organizações um pouco por todo o mundo e também em Portugal. Num estudo realizado em 2016 (Schulze, 2016) estima-se que, em termos mundiais, metade das entidades empregadoras vão preferir o BYOD em 2017, e que em 2018 serão usados cerca de 12.1 bilhões de dispositivos móveis.

A implementação de uma solução BYOD não é simples ou pacífica, sendo que a maioria das organizações optam por deixar acontecer em vez de agir, isto é, consentem a utilização dos dispositivos pessoais no acesso aos dados corporativos sem efetuarem uma avaliação dos impactos de segurança ou das necessidades de mudança na infraestrutura (IDC Portugal, 2015). Um outro estudo (Forrester Research, Inc., 2012) revela que poucas organizações que implementaram o modelo de ICT baseado em soluções BYOD mediram o impacto financeiro dessa implementação, e ainda menos conseguiram ter uma visão clara do significado do BYOD para o negócio.

Apesar de existirem benefícios consideráveis na adoção de uma solução BYOD, também existem ameaças que estão fora do âmbito e das medidas de controlo da segurança ICT. Ao propagarem-se os dados corporativos pelos dispositivos pessoais dos colaboradores, o perímetro de segurança dos dados das organizações estende-se igualmente para esses dispositivos. A grande variedade de dispositivos móveis, a falta de medidas de segurança adequadas aos dispositivos e o facto de esses dispositivos poderem ser facilmente partilhados aumenta o tipo de ameaças (Rivera et al. 2013). Sendo assim, é urgente que as organizações avaliem a viabilidade de uma solução

BYOD, a necessidade de aplicar controlos específicos, de estabelecerem uma gestão de políticas de segurança, e de executarem monitorização específica ao ambiente BYOD.

A gestão do risco assume um papel crucial na análise ou adoção do BYOD. De acordo com as conclusões de um estudo realizado pela KPMG (2013), metade das empresas portuguesas deram maior relevância aos riscos financeiros em detrimento dos riscos relacionados com a segurança das infraestruturas e equipamentos, sendo que uma percentagem admitiu que desenvolveu práticas de gestão do risco "*menos robustas no que respeita a modelo de governo, identificação e avaliação de riscos, monitorização, reporte e otimização da gestão do risco*". O estudo revela ainda que a maior parte das empresas portuguesas pretende reforçar a gestão do risco nos próximos anos.

1.2 Objetivos

O principal objetivo desta dissertação é providenciar uma ferramenta de suporte à decisão para avaliação de soluções BYOD e para tal começou-se por realizar uma análise geral das questões relacionadas com a implementação do BYOD em ambientes corporativos, tendo como suporte a avaliação e gestão de risco necessárias num contexto de governação e gestão. Uma das questões mais pertinentes é: Q1. Qual a metodologia de Análise e Gestão de Risco a seguir?

Pretende-se igualmente alertar para a necessidade das organizações procederem a uma análise que demonstre a viabilidade financeira da solução BYOD, colocando-se a questão: Q2. Que indicadores financeiros devem ser considerados que demonstrem a viabilidade da solução BYOD?

Esta dissertação tem ainda como objetivo contribuir de forma positiva para a identificação de boas práticas no que concerne à utilização do BYOD, num contexto, legal, corporativo e financeiro, pelo que foram equacionadas as questões:

Q3. Requisitos legais que podem influenciar a solução BYOD?;

Q4. Que riscos estão presentes na implementação de uma solução BYOD?;

Q5. Quais os benefícios e custos presentes na solução BYOD?;

Q6. O que considerar na elaboração de uma Política de Segurança BYOD?

1.3 Contribuições

A principal contribuição desta dissertação foi a criação de um modelo de suporte à decisão para avaliação da solução BYOD composto por vários modelos, nomeadamente

por um modelo: 1) de análise dos requisitos legais obrigatórios (MRLO); 2) de avaliação dos riscos (MAR) baseado na análise dos ativos e das potenciais ameaças; 3) de posicionamento ICT (MPICT) face aos controlos de segurança e/ou medidas de mitigação implementadas ou a implementar; 4) de análise relacionada com custo-benefício (MCBA) da solução BYOD; e 5) de estabelecimento da Política de Segurança BYOD (MCPSB).

Como plataforma de implementação, optou-se pelo Microsoft Office Excel devido a ser uma ferramenta com um interface intuitivo usada pela maior parte dos gestores e como tal de aprendizagem e utilização bastante eficaz e rápida.

1.4 Organização do documento

O trabalho foi estruturado em cinco capítulos sendo o Capítulo 1, Introdução, relacionado com a apresentação do tema, a motivação, os objetivos a atingir e a organização da dissertação.

O Capítulo 2, Gestão de Risco em SI, refere-se à pesquisa desenvolvida relacionada com os conceitos de gestão e avaliação de risco que permitiram contextualizar o tema do risco. Na seção Metodologias de Gestão e de Risco são apresentadas as principais metodologias de suporte à Gestão do Risco. Na seção Análise Financeira são referidos conceitos financeiros que podem ser aplicados num contexto de suporte financeiro à implementação do BYOD. Este capítulo responde as questões Q1 e Q2.

No Capítulo 3, Análise a soluções BYOD, é realizada uma análise dos potenciais problemas de segurança e dos mecanismos de controlo disponíveis, assim como o enquadramento do BYOD segundo uma perspetiva legal. Neste capítulo são respondidas as questões Q3, Q4, Q5 e Q6 através da avaliação das vantagens e desvantagens da implementação da solução BYOD, os potenciais riscos e, as soluções que permitem reduzir os riscos para níveis aceitáveis.

No Capítulo 4, Modelo de suporte à decisão para apreciação de solução BYOD, é proposto o modelo de suporte à decisão para avaliação de soluções BYOD, composto por diversos modelos.

No Capítulo 5, Conclusão, são apresentadas as conclusões e propostas para a realização de trabalho futuro.

Capítulo 2

Gestão de Risco em SI

No âmbito da implementação BYOD foi efetuado o estudo de diferentes metodologias de gestão de risco e os principais métodos de análise financeira de forma a enquadrar a necessidade das organizações executarem um trabalho prévio nessas áreas, caso optem por uma solução BYOD.

O BYOD já está presente em muitas organizações independentemente do tamanho da organização ou do sector. Já é bastante comum os colaboradores utilizarem os dispositivos pessoais ao serviço das organizações, por exemplo na consulta do correio eletrónico, na construção de documentos, na consulta dos dados empresariais, etc. Se por um lado incorpora benefícios para as organizações, como por exemplo na poupança de custos e na satisfação dos colaboradores – traduzindo-se em aumento de produtividade, também incorpora riscos, pelo que importa determinar esses riscos.

Em traços gerais, a gestão incorreta do risco pode ser definido como a possibilidade ou a probabilidade de algo ocorrer relacionado com situações adversas que podem causar problemas ou danos. Sendo assim, é necessário avaliar e determinar a melhor maneira de gerir o risco. No entanto e, porque envolve sempre um grau de incerteza, nem sempre é possível avaliar todos os aspetos do risco e obter todas as consequências relacionadas com as medidas de controlo implementadas. A gestão do risco permite avaliar o risco, determinar a sua complexidade e esclarecer dúvidas e lacunas.

"You can't effectively and consistently manage what you can't measure, and you can't measure what you haven't defined..."[1]

[1] Citação «*An Introduction to Factor Analysis of Information Risk (FAIR)*», (Jones, 2005)

2.1 Gestão do Risco

De acordo com a norma internacional ISO 31000:2013 (ISO, 2013), o risco pode ser definido como o efeito (desvio do esperado, podendo ser positivo e, ou negativo) da incerteza sobre os objetivos (que podem ter diferentes aspetos - financeiro, de segurança, ambientais, etc., aplicados a diferentes níveis - estratégicos, organizacionais, de projetos, produtos, etc.). Pode ser caracterizado por referência a potenciais eventos e consequências, ou a uma combinação de ambos. Pode ser expresso como a combinação das consequências de um evento, associado à verosimilhança da ocorrência, sendo o valor da verosimilhança associado à estimativa de probabilidade, pelo que o termo probabilidade será usado para representar essa estimativa.

A análise do risco, por sua vez, é o processo que irá permitir identificar as ameaças, vulnerabilidades e ativos, documentar e identificar medidas de mitigação e avaliá-las. Sendo assim o valor do risco pode ser estimado pela probabilidade de uma vulnerabilidade ser explorada com sucesso por uma dada ameaça multiplicada pelo valor da informação do ativo menos a percentagem de risco mitigado por controlos correntes mais a incerteza do conhecimento (Whitman & Mattord, 2010).

A utilização de uma metodologia de gestão do risco permite estabelecer regras quanto ao que se pretende avaliar, quem necessita de ser envolvido, a terminologia usada na discussão do risco, os critérios de quantificação e qualificação, a comparação de níveis de risco e a documentação que é necessária recolher e produzir como resultado da avaliação e da continuidade das atividades de avaliação do risco. A finalidade é medir objetivamente o risco permitindo que as organizações consigam quantificar e qualificar o risco do negócio em relação a informações e ativos críticos.

É primordial que as organizações, nas suas análises, estabeleçam uma visão temporal dos riscos. Existem os riscos correntes, que são os riscos atuais que ameaçam os ativos no presente e, sobre os quais é necessário agir de forma imediata. Existem os riscos emergentes, isto é, riscos que, dependendo de várias circunstâncias (como por exemplo, de alterações da conjuntura socioeconómica, do próprio âmbito de atuação, da implementação de medidas de mitigação, etc.) podem ocorrer. E, existem os riscos futuros, ou seja, os riscos previsíveis num futuro próximo, sobre os quais pesam sobretudo as tomadas de decisão que podem atenuar os mesmos. Na Figura 2.1, a

ENISA[2] quantifica o tempo com base na análise do tipo de risco: os riscos correntes como riscos atuais; os riscos emergentes como riscos que podem ocorrer no espaço de um ano e, os riscos futuros, os que podem decorrer no espaço de cinco anos.

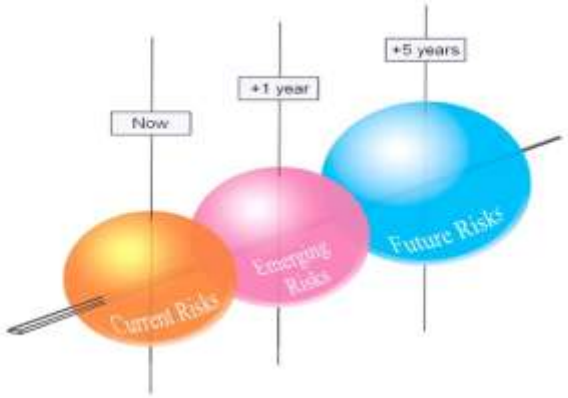

Figura 2.1 - Risco - Visão temporal (ENISA, 2015)

Em termos de atividade, existem alguns passos fundamentais na gestão de riscos. *The MITRE Corporation* (Mitre, 2014)[3], resume a gestão do risco em quatro passos fundamentais (Figura 2.2), que consistem na:

1) Identificação do Risco;
2) Avaliação do Impacto/Consequências do Risco (como por exemplo custos, calendário ou objetivos de desempenho técnicos, etc.);
3) Análise da Priorização do Risco, nomeadamente a identificação de riscos críticos e de riscos menos críticos e,
4) Plano de Mitigação do Risco, Implementação e Monitorização Contínua, considerando não só a gestão, eliminação e redução do risco para níveis aceitáveis, como atividades de monitorização contínua que permitam revisitar as ações definidas, em caso de necessidade. Adicionalmente referem mais dois passos:
    i) O desenvolvimento de uma abordagem e de um plano – determinação dos processos, das técnicas, dos responsáveis e da estrutura do projeto e,

[2] ENISA, *European Union Agency for Network and Information Security* ou Agência Europeia para a Segurança das Redes e da Informação é um organismo da União Europeia que visa ajudar a responder a problemas de cibersegurança através de ações de sensibilização e da promoção das melhores práticas e do conhecimento na área da segurança da informação.

[3] The Mitre Corporation é uma organização americana não lucrativa, formada em 1958, que gere os diversos centros federais de pesquisa e de desenvolvimento americanos (*Federally Funded Research and Development Centers - FFRDCs*) suportados por sua vez por vários organismos americanos.

ii) A seleção da ferramenta de gestão do risco – relacionado com a implementação e execução do programa de gestão de risco, tendo em conta a complexidade e os recursos disponíveis.

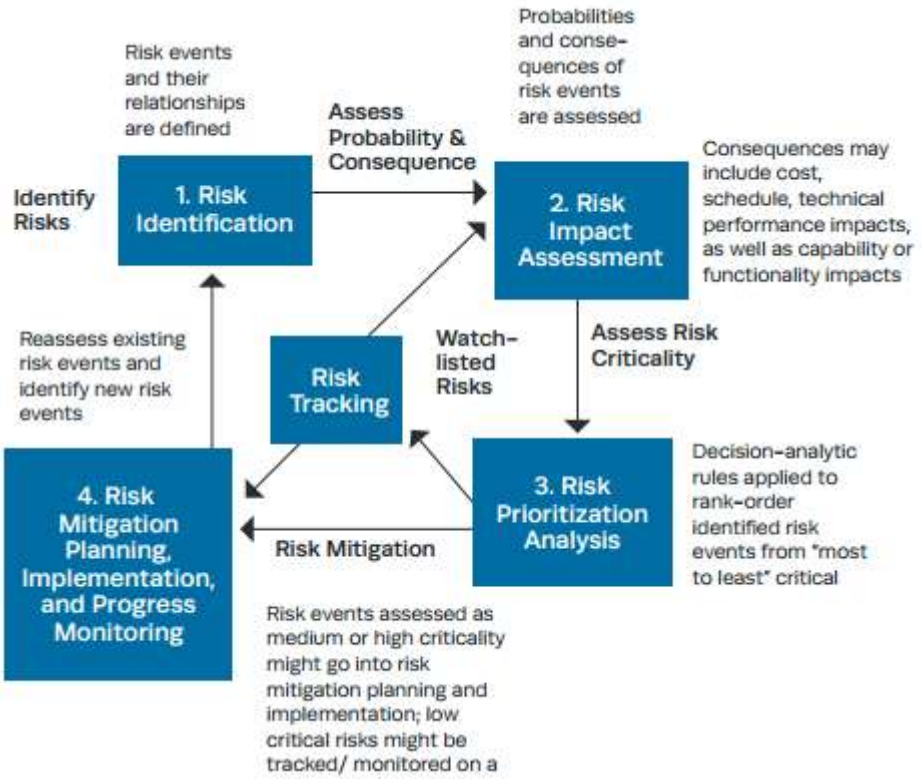

Figura 2.2 - Gestão do Risco - Passos fundamentais (MITRE, 2014)

Em termos de processo, a gestão do risco é visto como um ciclo composto por diferentes processos, conforme ilustra a Figura 2.3 que representa a visão proposta pela ENISA, organizado segundo as diretrizes da ISO 27005:2011 (ISO/IEC, 2011). Cada processo avalia uma parte que no todo compõe a gestão do risco. O primeiro processo relaciona-se com a Estratégia Corporativa da Gestão do Risco. Neste processo é efetuado a definição dos objetivos do âmbito e da metodologia de avaliação de risco. Integra dois processos: definir a metodologia do processo gestão de risco e os canais de comunicação da organização (delineado na Figura 2.3 pela zona amarela). No processo de Avaliação do Risco considera-se a identificação do risco, a análise de riscos relevantes, onde também é definido o tipo de análise (qualitativa, semi-quantitativa ou quantitativa) e a avaliação do risco. O processo seguinte, Tratamento do Risco, consiste em selecionar e implementar medidas para modificar o risco. Neste passo são consideradas as opções, como por exemplo, evitar, otimizar, transferir ou reter o risco; o desenvolvimento de planos; a aprovação e a implementação de planos de ação e, a identificação de riscos residuais. O processo Aceitação do Risco consiste na aceitação

de riscos residuais como resultado do processo de Tratamento do Risco e do processo de Comunicação dos riscos residuais aos decisores. Apesar de indicado como processo opcional, uma vez que encontra-se implícito nos outros processos, é mencionado com o intuito de se conseguir um compromisso por parte dos gestores, evitando que seja interpretado como uma mera atividade de comunicação. Por último o processo de Monitorização e Revisão dos processos alerta para a necessidade do processo de gestão de risco ser um processo cíclico e regular, e onde devem ser revistos os planos de ação de forma a manterem-se relevantes e atualizados. Com base nestes processos as organizações conseguem executar com eficiência e efetividade do processo de Gestão do Risco.

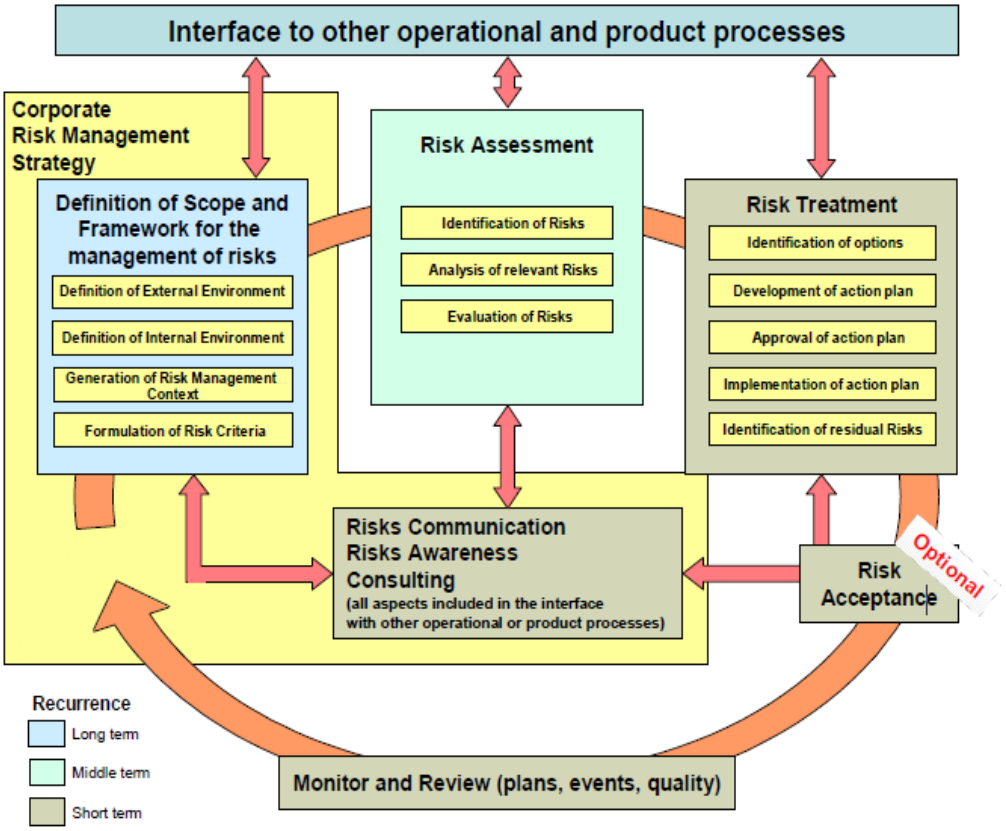

Figura 2.3 - Gestão do Risco - Visão geral do processo (ENISA, 2006)

Ainda e, de acordo com a ENISA, podemos observar a relação entre Gestão e a Avaliação do Risco, baseado na metodologia OCTAVE (Figura 2.4).

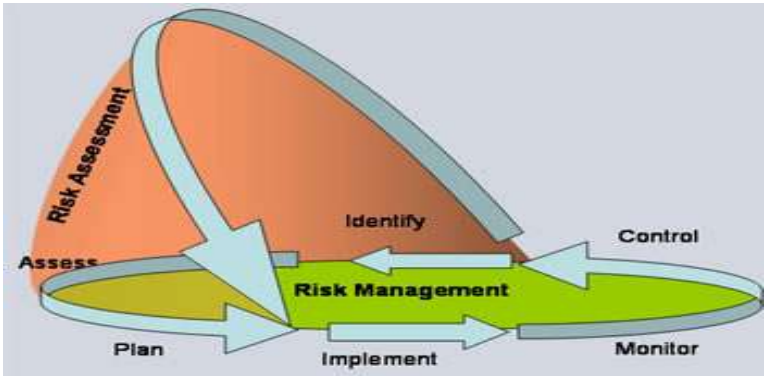

Figura 2.4 - Relação gestão vs. Avaliação do risco (ENISA, 2006)

A Gestão do Risco pode ser definida como uma atividade recorrente que engloba o planeamento, a implementação, a monitorização e o controlo das medidas e das políticas de segurança implementadas, sendo a Avaliação do Risco executada em determinada altura (seja anualmente, a pedido, etc.) do processo, e até à próxima iteração, na identificação e avaliação dos riscos fornecendo assim uma visão sobre a parametrização de todo o processo de Gestão do Risco.

O tratamento do risco é a aplicação sistemática de políticas, procedimentos e práticas de gestão que permitem estabelecer o contexto e identificar, analisar, eliminar ou mitigar para um nível aceitável, os perigos e consequentemente os riscos que possam ameaçar a organização. No entanto, nem todos os riscos podem ser eliminados e nem todas as medidas de mitigação são economicamente exequíveis. Nesse sentido, o recurso a modelos de avaliação de risco de forma periódica é uma mais-valia no suporte à gestão do risco.

2.2 Avaliação do Risco

A avaliação do risco é um processo que deve ser realizado, independentemente da implementação da gestão de risco. Através da avaliação do risco são identificadas, analisadas e avaliadas as ameaças e as vulnerabilidades sendo possível entender e medir o impacto do risco envolvido e assim decidir sobre as medidas e controlos mais adequados. O recurso a *frameworks* permite estabelecer não só regras sobre o que se pretende avaliar, como identificar quem necessita de ser envolvido, qual a terminologia a usar na discussão dos riscos, os critérios de quantificação e de qualificação, a comparação dos níveis de risco, assim como a documentação que deve ser recolhida e produzida como resultado da avaliação e das atividades de continuação, ou seja, de *follow-up*. As *frameworks* pretendem estabelecer medidas objetivas sobre o risco

fazendo com que as organizações entendam em termos qualitativos e quantitativos qual o risco do negócio em relação aos ativos críticos. As metodologias de avaliação de risco fornecem as ferramentas necessárias para a tomada de decisões (exemplo dos investimentos necessários ou mais adequados), uma vez que objetivam direcionar o risco para um nível aceitável.

2.3 Metodologias de Gestão e de Risco

Um dos desafios das organizações está em selecionar uma metodologia de gestão do risco de segurança da informação robusta e em conformidade com os objetivos de controlo. Existem disponíveis diversas *frameworks* conforme podemos verificar na avaliação feita pela ENISA (2006) e por CESG (2015). Todas têm uma abordagem similar sendo no entanto diferentes quer nos objetivos de alto nível, quer na linguagem utilizada como podemos verificar de seguida.

2.3.1 *COBIT 5*

O COBIT *(Control Objectives for Information and Related Technology)* é uma metodologia desenvolvida pelo ISACA (ISACA, 2015)[4] referente à gestão e governação IT. Surgiu em 1996, tendo vindo a evoluir em termos de áreas de atuação (Figura 2.5), consoante as necessidades e os desafios presentes nas organizações.

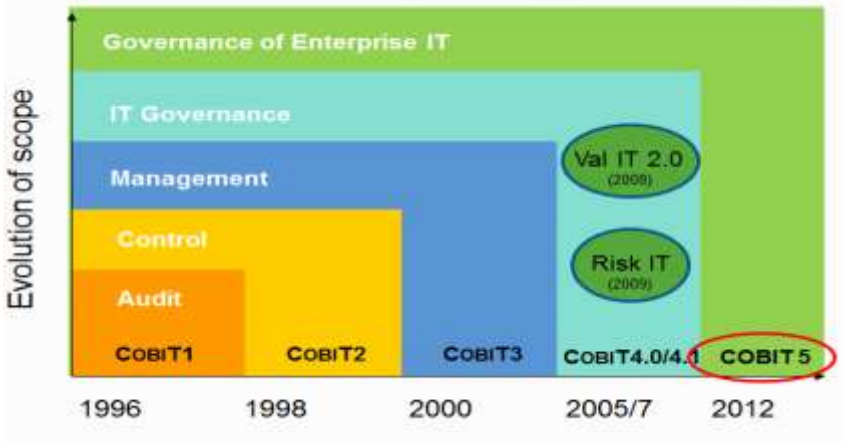

Figura 2.5 - COBIT - Evolução (ISACA, 2012a)

[4] Associação global não lucrativa estabelecida em 1969, anteriormente conhecida como *Information Systems Audit and Control Association*, atualmente é constituída por 140.000 profissionais em 180 países. Inclui membros como auditores internos e externos, *CEOs*, *CFOs*, *CIOs*, profissionais de segurança e de controlo da informação, investigadores, académicos, gestores de negócio, estudantes e consultores de IT.

Lançado em junho de 2012, o COBIT 5 aborda requisitos de controlo, problemas técnicos e riscos de negócio. Consolida e integra o COBIT 4.1[5], os modelos de processos Val IT 2.0[6] e o RISK IT[7], conforme podemos observar na Figura 2.6.

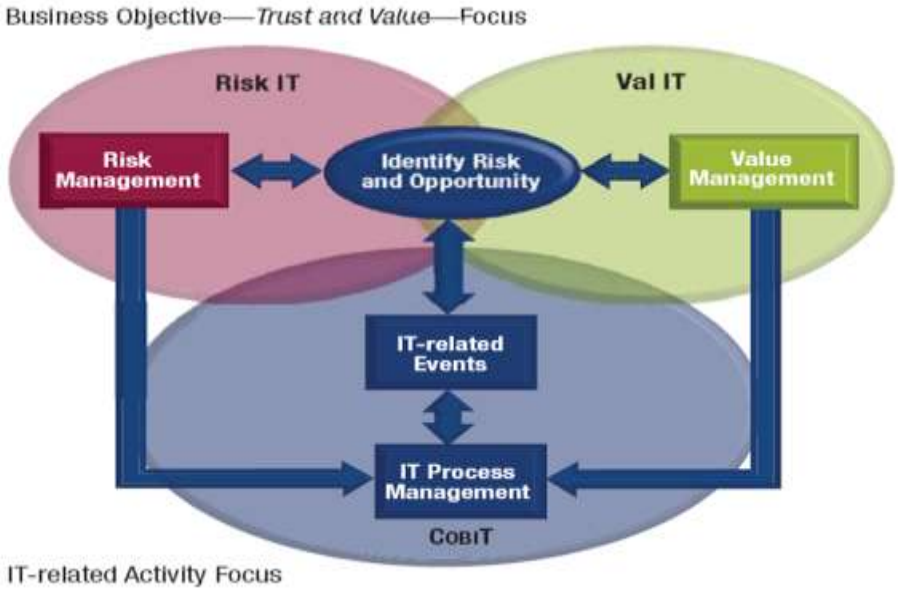

Figura 2.6 - COBIT, RISK IT e VAL IT - Integração (ISACA, 2009)

O COBIT 4.1 estabelece um conjunto de boas práticas para a gestão do risco através da definição de um conjunto de controlos que permitem mitigar riscos IT. O RISK IT complementa o COBIT na identificação, governação e gestão de riscos IT, e o VAL IT adiciona-lhe a perspetiva financeira do negócio.

O COBIT 5 apresenta uma maior maturidade principalmente na área relacionada com a segurança da informação e os riscos, sendo uma mais-valia nas questões de gestão da informação e da governança IT e, em questões de conformidade com requisitos legais e regulações externas.

---

[5] COBIT 4.1, lançado em maio de 2007, consiste num modelo de processos que subdivide o IT em quatro domínios: Planeamento e Organização (*Plan and Organise - PO*), Adquisição e Implementação (*Acquire and Implement - AI*), Entrega e Suporte (*Delivery and Suport - DS*), Monitorização e Avaliação (*Monitor and Evaluate - ME*) e, em 34 processos relacionados as áreas de responsabilidade de planeamento, instalação, execução e monitorização.

[6] Val IT, desenvolvido pelo *IT Governance Institute* (ITGI), é uma metodologia de governação com o intuito de criar valor de negócio aos investimentos de IT. Consiste na definição de princípios orientadores, de um conjunto de processos e boas práticas referente a práticas de gestão, servindo assim de suporte e apoio aos gestores das organizações

[7] RISK IT, desenvolvido pelo ISACA em 2009 tem como objetivo estabelecer uma visão *end-to-end* completa dos riscos relacionados com a utilização de IT e uma solução similar em relação à gestão de tratamento do risco, abordando não só a cultura de topo como as questões operacionais. É composto por três processos/domínios: Governação do Risco, Avaliação do Risco e Resposta ao Risco, cada processo contêm por sua vez uma série de atividades.

O COBIT 5 é composto por uma família de produtos (Figura 2.7) nomeadamente pelo modelo COBIT 5, por *Enabler Guides* ou guias facilitadores, por Guias Profissionais e por um ambiente *online* colaborativo de suporte ao COBIT 5.

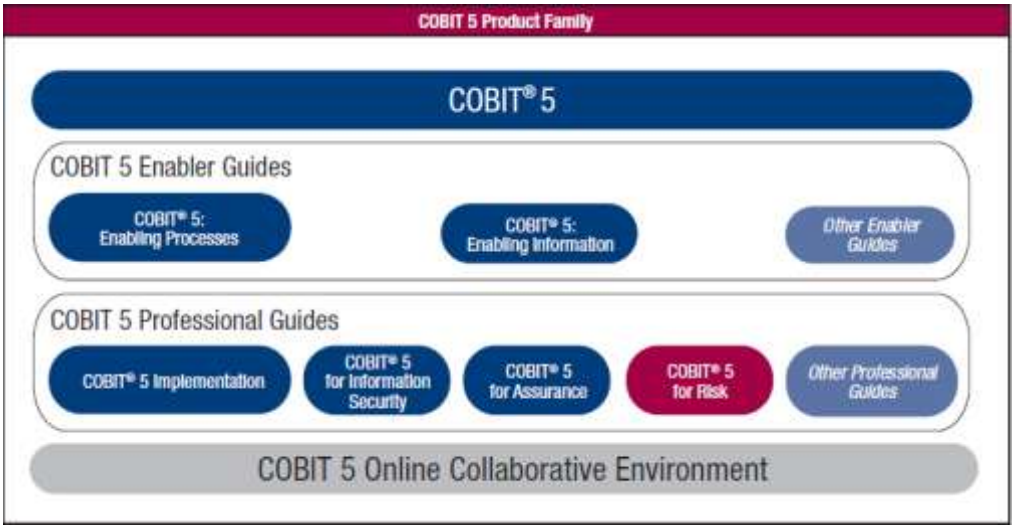

Figura 2.7 - COBIT 5 – Família de produtos COBIT 5 (ISACA, 2012b)

No COBIT 5 são definidos cinco princípios (Figura 2.8):

1. Ir ao encontro das necessidades dos *stakeholders*;
2. Considerar a organização no seu todo;
3. Aplicar uma metodologia única integrada;
4. Permitir uma abordagem holística e
5. Separar a governança da gestão.

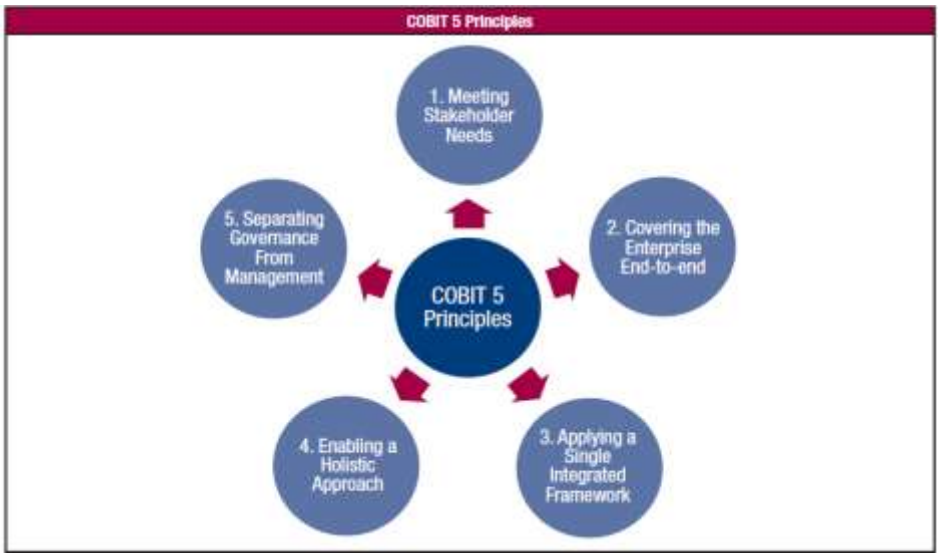

Figura 2.8 - COBIT 5 – Princípios (ISACA, 2012b)

O estabelecimento desses princípios tem como objetivo permitir que as organizações estabeleçam uma estrutura de governação e gestão efetiva baseada numa

visão holística otimizando assim os investimentos na informação e na tecnologia, aumentando a confiança dos *stakeholders.*

Considerando os princípios e o respetivo contexto, o COBIT 5 descreve diferentes facilitadores de suporte aos princípios. Os facilitadores devem ser desenvolvidos à medida das necessidades das organizações e servem de guias orientadores na percussão dos objetivos da organização. No COBIT 5 são estabelecidos sete categorias de facilitadores (Figura 2.9):

1) Princípios, Políticas e Metodologias, relacionando com as orientações da gestão;
2) Processos, direcionado para o conjunto de práticas e atividades estabelecidos pela organização com o intuito de atingir os objetivos pretendidos;
3) Estrutura Organizacional, relacionado com as principais áreas de tomada de decisão da organização;
4) Cultura, Ética e Comportamentos, como fator decisivo também para o sucesso das organizações;
5) Informação, no que refere à gestão da informação;
6) Serviços, Infraestruturas e Aplicações, dirigido sobretudo aos processos de suporte da informação;
7) Pessoas, Conhecimentos e Competências, enquadramento em termos de necessidades organizacionais.

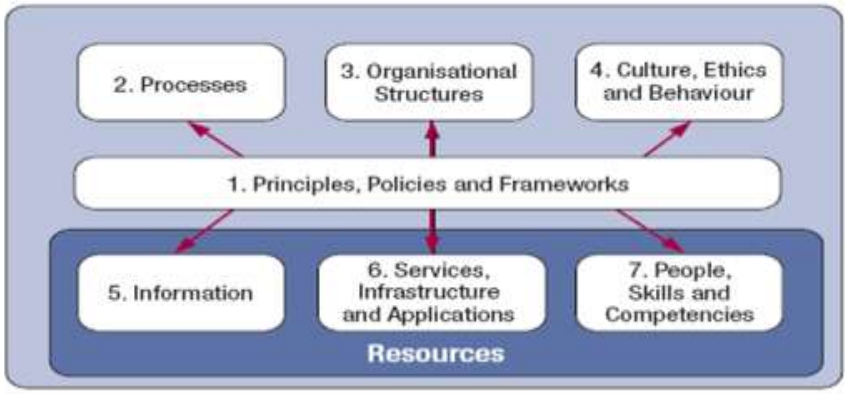

Figura 2.9 - COBIT 5 – Enablers (ISACA, 2012b)

Com base na metodologia COBIT 5 são disponibilizados alguns guias profissionais. O guia *COBIT 5 for Risk* dirigido às questões e problemas fundamentais da gestão de riscos IT, integra os facilitadores do COBIT 5 acima referidos. É composto por três seções:

A primeira seção, Gestão do Risco e o Risco (*Risk and Risk Management*) relaciona-se com orientações ao nível do risco e descreve como aplicar os princípios do COBIT 5 às necessidades específicas da gestão do risco. Levantamento das opiniões consistentes e fundamentadas dos *stakeholders* em relação ao risco atual; orientação de como gerir o risco para níveis dentro do apetite de risco da organização; orientação de como configurar a cultura de risco adequada e, a possibilidade de executar avaliações de risco quantitativas que permitam aos interessados considerar o custo de mitigação e os recursos necessários contra a exposição à perda.

A segunda seção, refere-se à perspetiva do risco, considerando a aplicação prática dos facilitadores. Subdivide-se na 2a) Perspetiva da Função do Risco (*The Risk Function Perspective*) e na 2b) Perspetiva da Gestão do Risco (*The Risk Management Perspective*). A Perspetiva da Função do Risco e, recorrendo aos facilitadores do COBIT 5, descreve como construir e manter a função de risco na organização. Considera sete princípios (Figura 2.10) providenciado uma abordagem estruturada e sistemática do risco. Permite aplicar na prática os princípios e, avaliar a sua influência nas tomadas de decisão.

Figura 2.10 - COBIT 5 *For Risk* – Princípios (ISACA, 2013)

Ainda nesta subseção são identificados os processos do COBIT 5 necessários no suporte à função do risco. À semelhança do COBIT 4, são considerados quatro domínios com ligeiras alterações. Assim temos o modelo de processos que subdivide o IT em: i) Alinhamento, Planeamento e Organização (*Align, Plan and Organise - APO*), ii) Construção, Adquisição e Implementação (*Build, Acquire and Implement - BAI*), iii) Entrega, Serviço e Suporte (*Delivery, Service and Suport - DSS*) e iv) Monitorização, Avaliação e Acesso (*Monitor, Evaluate and Assess - MEA*). Na Figura 2.11, os

processos estão estabelecidos de acordo com os quatro domínios, ou seja, os processos de suporte chave (rosa escuro); outros processos de suporte (rosa claro), e os processos de risco centrais (azul claro - AP012 e EDM03).

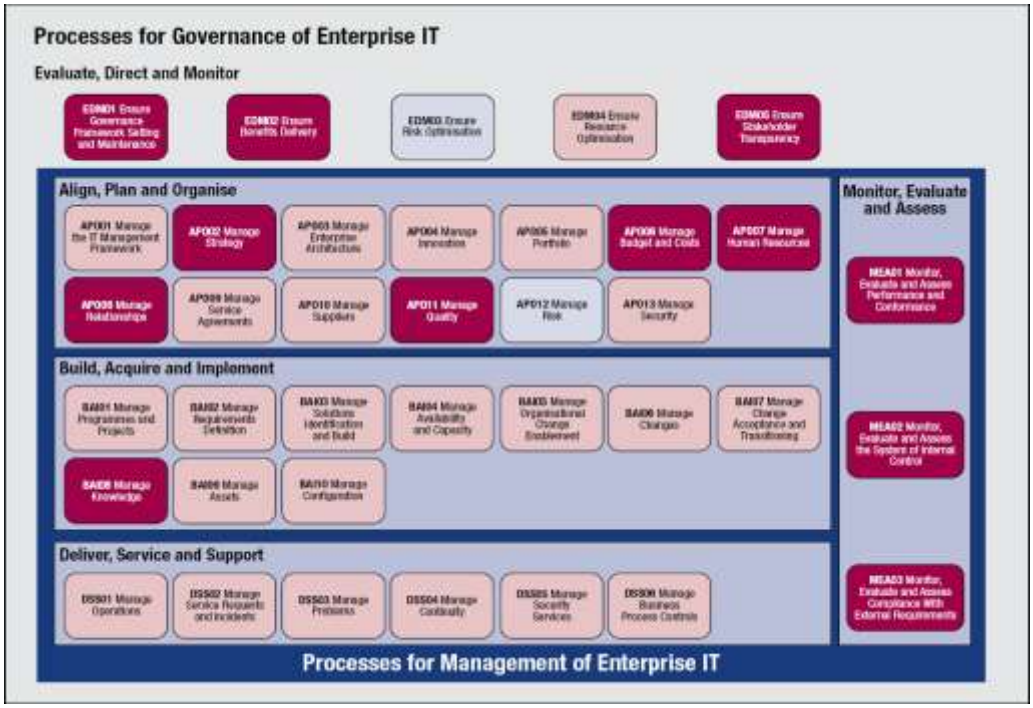

Figura 2.11 - COBIT 5 For Risk – Processos (ISACA, 2013)

Na subseção da Perspetiva da Gestão do Risco é considerado a governação do risco, o processo do risco e cenários de risco. Aplicando os facilitadores do COBIT 5, são descritas formas de mitigação do risco. Na Figura 2.12 podemos verificar a perspetiva do risco de acordo com o COBIT 5 *For Risk.*

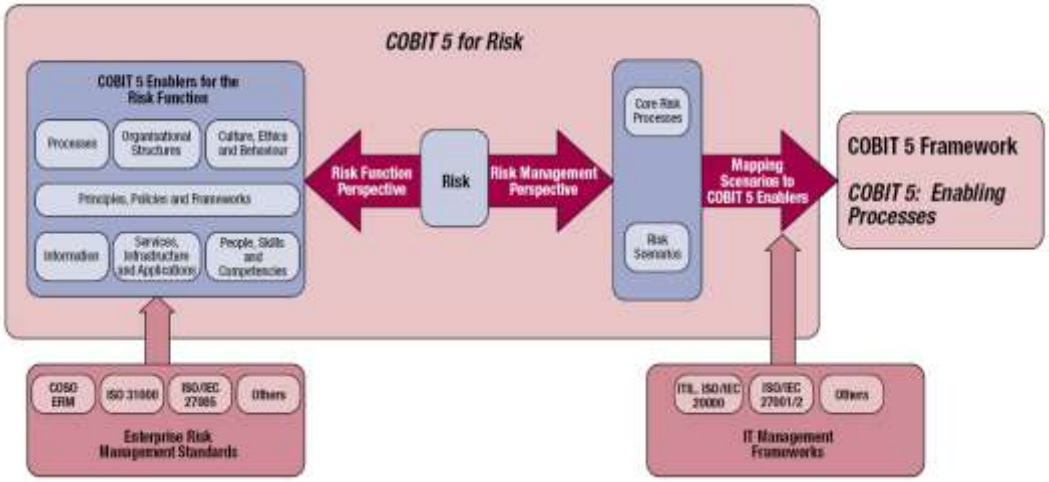

Figura 2.12 - COBIT 5 *For Risk* – Âmbito (ISACA, 2013)

A terceira seção considera o alinhamento e a relação do *COBIT 5 For Risk* com outros padrões relevantes de IT e de ERM.

Os princípios e os facilitadores do COBIT 5 são genéricos e úteis para todo o tipo de organizações, comerciais, não-lucrativas ou mesmo para o setor público. O COBIT 5 integra com outras metodologias como o ITIL, a ISO 31000:2013 (ISO, 2013) e a ISO 27005:2011 (ISO/IEC, 2011), o PMBOK (*Project Management Body of Knowledge*), o PRINCE2 (*Project in Controlled Enviroments*) e o TOGAF (*The Open Group Architecture Framework).*

2.3.2 *FAIR*

FAIR ou *Factor Analysis of Information Risk* é uma metodologia desenvolvida por Jack Jones da *Risk Management Insight LLC* (Jones, 2005) com o intuito de perceber, analisar e medir o risco da informação.

Considerado como um padrão internacional pelo *The Open Group*[8] (The Open Group, 2013) a FAIR recorre ao modelo VAR ou VaR (*Value at risk* ou valor em risco) no que concerne à segurança da informação e aos riscos operacionais. A sua principal preocupação é quantificar a informação e o risco operacional em termos financeiros de forma a facilitar a tomada de decisões. O FAIR providencia uma metodologia que pode ser usada em conjunto com outros modelos de risco como COSO, ITIL, ISO/IEC 27005, ISO/IEC 31000, COBIT, OCTAVE, etc. (The Open Group, 2009), podendo reforçar e complementar esses modelos de análise de risco, em vez de substituí-los.

A metodologia FAIR parte de três fatores principais:

- O Valor do Ativo, segundo a visão do agente de ameaça;
- A Vulnerabilidade, ou seja, a expectativa de sucesso do agente de ameaça;
- O Risco, relacionado com a probabilidade de ocorrência e a provável magnitude de perda provocadas pelo agente de ameaça.

Na Figura 2.13 encontra-se representada a visão geral da taxonomia do risco de acordo com a metodologia FAIR. A taxonomia do risco é composta por dois ramos principais, designados por Frequência de Eventos de Perda (*Loss Event Frequency - LEF*) e por Magnitude de Perda Provável (*Probable Loss Magnitude - PLM*). A metodologia FAIR consiste em decompor em primeiro lugar os fatores que levam ao *LEF*, sendo cálculos relativamente simples porque possuem uma relação de causa efeito

[8] The Open Group é um consórcio global formado em 1996 aquando da fusão entre a X/Open e a Open Software Foundation. Possibilita a realização de objetivos de negócio através do estabelecimento de padrões de IT. É composto por diversos membros de diferentes organizações abrangendo todos os setores de IT, desde clientes, sistemas e soluções, fornecedores de ferramentas, consultores, académicos e investigadores.

e, de seguida examinar os fatores que levam à PLM, sendo estes fatores com relações mais complicadas medidos e estimados pela agregação do tipo de perdas.

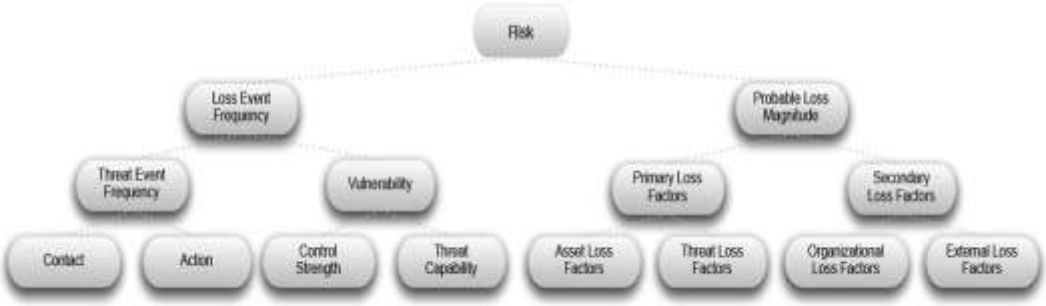

Figura 2.13 - FAIR - Taxonomia do risco (Risk Management Insight, 2006)

A análise FAIR básica é composta por dez passos em quatro fases. Os passos consistem em identificar e estimar os elementos nas caixas da Figura 2.13 utilizando uma abordagem *bottom – up.*

2.3.3 *ISO/IEC 27005:2011*

A ISO/IEC 27000 *series* é um conjunto de normas internacionais relacionadas com a segurança da informação publicadas pela ISO (*International Organization for Standardization*) e pelo IEC (*International Electrotechnical Commission*), onde a norma ISO/IEC 27005:2011 - *Information technology - Security techniques -- Information security risk management* (ISO/IEC, 2011), estabelece uma metodologia que providencia orientações para a gestão de riscos de segurança da informação.

A ISO/IEC 27005:2011 tem por objetivo dar suporte às orientações dos requisitos de criação, manutenção e de melhoria contínua dos sistemas de gestão de segurança da informação (SGSI ou *ISMS - Information Security Management System*) definidos na norma NP ISO/IEC 27001:2011 (ISO/IEC, 2013).

Esta norma é aplicável a todo o tipo de organizações e não fornece ou recomenda uma metodologia específica, sendo que a sua aplicação vai depender de uma série de fatores como o tipo ou o sector da organização.

A ISO/IEC 27005:2011 define o processo de gestão de risco da segurança da informação como um processo contínuo onde deve ser estabelecido o contexto, a avaliação e tratamento do risco através de um plano de tratamento de risco que permita implementar as recomendações e decisões. Através do processo de gestão de risco pretende-se analisar o que pode acontecer e, quais podem ser as possíveis consequências antes de decidir o quê e quando deve ser feito, de forma a reduzir o risco para um nível

aceitável. Sendo assim e, conforme podemos observar na Figura 2.14, o processo de gestão do risco da segurança da informação consiste em atividades coordenadas e iterativas entre si:

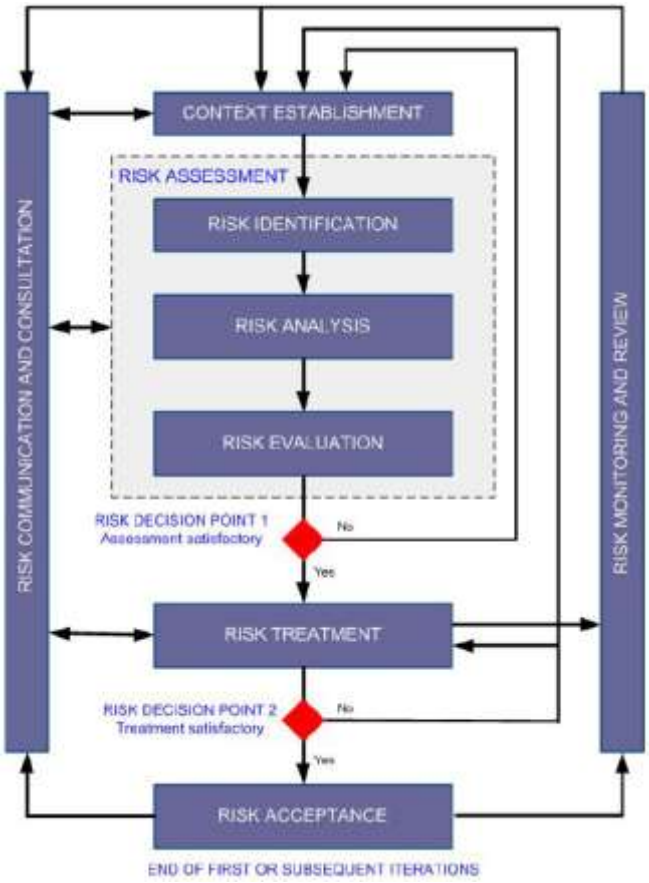

Figura 2.14 - Processo de gestão de riscos de SI (ISO/IEC, 2011)

A iteratividade entre as atividades permite um bom equilíbrio entre a minimização dos tempos e dos esforços despendidos na identificação dos controlos, assegurando igualmente a avaliação apropriada dos riscos de alto nível.

Analisando ao pormenor temos a primeira atividade - estabelecimento do contexto, que envolve definir os critérios básicos necessários para a gestão de risco da segurança da informação, nomeadamente os objetivos e os limites através do estabelecimento de critérios de avaliação de riscos, critérios de impacto e critérios de aceitação do risco. Nos critérios de avaliação de riscos há que considerar: i) o valor estratégico do processo de informação do negócio; ii) a criticidade dos ativos de informação envolvidos; iii) requisitos legais, regulatórios e, ou obrigações contratuais; iv) importância operacional e de negócio dos critérios de segurança: disponibilidade, confidencialidade e integridade; v) perceções e expectativas das partes interessadas

(*stakeholders*) e consequências negativas. Os critérios de avaliação de risco podem ser usados para especificar as prioridades na atividade de tratamento de risco.

A questão dos critérios de impacto deve ser desenvolvida e especificada em termos de grau do dano ou de custos para a organização causados por eventos de segurança da informação tendo em conta: i) o nível de classificação do impacto do ativo na informação; ii) violações à segurança da informação (isto é, perda de confidencialidade, integridade e disponibilidade); iii) operações deficitárias; iv) perda de negócio e de volume financeiro; v) disrupção de planos e de prazos; vi) danos na reputação; vii) violações de requisitos legais, regulatórios ou contratuais.

Os critérios de aceitação do risco dependem das políticas da organização, das metas, dos objetivos e dos interesses dos *stakeholders*. As organizações devem definir os seus próprios níveis de aceitação de risco, tendo em consideração: i) a inclusão de múltiplos limites, com o nível de risco desejado, identificando igualmente a possibilidade de aceitação do risco acima desse nível em determinadas circunstâncias; ii) o rácio de lucros estimados (ou outros benefícios de negócio) para o risco estimado; iii) o estabelecimento de diferentes critérios de aceitação de risco para diferentes classes de risco, isto é, determinados tipo de riscos não aceitáveis (por exemplo do tipo regulatórios ou legislativos) e outros aceitáveis (exemplo, os mencionados em requisitos contratuais); iv) os requisitos de tratamento do risco, ou seja, a redução do risco para um nível aceitável definido por um determinado período de tempo. Os critérios de aceitação de risco podem diferir consoante é expectável o risco existir, pelo que deve ser tido em conta o critério do negócio, aspetos legais e regulatórios, operações, tecnologias, finanças e fatores sociais e humanitários.

Ainda, na primeira atividade importa definir os objetivos e os limites a considerar na gestão de risco da segurança da informação garantindo assim a identificação de todos os ativos relevantes, assim como os limites que permitem direcionar os riscos que possam surgir. Adicionalmente devem ser registadas as justificações das exclusões dos objetivos. Por último, importa igualmente definir a organização, a aprovação e as responsabilidades do processo de gestão de risco da segurança da informação.

A apreciação de risco permite não só quantificar ou qualificar o risco como habilitar os gestores a priorizarem o risco de acordo com a perceção da seriedade ou de outro critério entretanto estabelecido. A apreciação do risco consiste nas atividades de: i) identificação do risco, ii) análise de risco e iii) avaliação do risco. Assim, a identificação do risco tem como propósito determinar o que pode causar uma potencial

perda, como pode acontecer, onde e porquê pode acontecer a perda. É necessário identificar: i) os ativos com valor para a organização, os que requerem proteção, e os seus responsáveis; ii) as ameaças, os tipos e as suas origens; iii) a existência e o planeamento de controlos, suas implementações e respetivos estados; iv) vulnerabilidades em relação aos ativos, ameaças e controlos; v) consequências operacionais através de cenários de incidentes relacionados com os ativos e os processos de negócio (exemplo, consequências relacionadas com a perda de confidencialidade, integridade e disponibilidade). Na Análise de Risco são estabelecidos critérios de i) avaliação de risco, ii) critérios de impacto e iii) critérios de aceitação de risco. Na avaliação do risco, o nível de risco deve ser comparado com os critérios de avaliação de risco e os critérios de aceitação produzindo-se dessa forma uma lista de riscos priorizada de acordo com os critérios de avaliação do risco em relação aos cenários de incidentes que levam a esses riscos.

Com base nos dados da avaliação dos riscos e desde que a avaliação seja satisfatória (ponto de decisão um, presente na Figura 2.14), isto é, adequada conforme os critérios estabelecidos, segue-se para a atividade de tratamento do risco. Esta atividade tem como objetivo definir um plano de tratamento do risco através da identificação de controlos que permitam reduzir, reter, evitar ou transferir o risco para um nível de risco residual aceite pelos gestores da organização. Nesta atividade e, à semelhança da anterior, considera-se a possibilidade de reiniciar-se a mesma (ponto de decisão dois, presente na Figura 2.14) até ao estabelecimento de riscos residuais satisfatórios a serem aceites pelos gestores da organização.

A atividade de aceitação do risco engloba o registo formal das decisões de aceitação do risco e da responsabilidade pela decisão. Deve incluir não só o plano de tratamento do risco assim como a lista de riscos aceitáveis com justificação e, que não estão de acordo com os critérios de aceitação do risco, ou seja, as decisões aceites na avaliação do risco residual.

A atividade de comunicação do risco tem como objetivo permitir a troca e partilha da informação entre os decisores e outros *stakeholders* da informação obtida no decorrer das atividades desenvolvidas no processo de gestão do risco.

A atividade de monitorização e revisão do risco consiste em monitorizar e rever continuamente os riscos e os fatores relacionados (isto é, o valor dos ativos, os impactos, as ameaças, as vulnerabilidades, a probabilidade de ocorrência) de forma a

identificar eventuais alterações de contexto, assim como manter a visão do risco o mais completa e atual possível através de atualizações contínuas.

2.3.4 *NIST SP 800-30*

NIST Special Publications (SPs) são publicações desenvolvidas e emitidas pelo *National Institute of Standards and Technology (NIST),* com o intuito de emanarem recomendações e orientações relacionadas com a segurança da informação.

O *NIST Special Publications 800-30* "*Guide for Conducting Risk Assessments*" **(**NIST, 2012), refere-se a uma visão de alto nível do processo de avaliação de risco, onde são documentadas passo a passo: i) as atividades necessárias de preparação da avaliação; ii) as atividades necessárias de condução efetiva da avaliação do risco; iii) as atividades necessárias de comunicação da avaliação de resultados e, iv) as atividades necessárias de manutenção dos resultados de avaliação de risco numa base de continuidade (*ongoing*). O documenta considera quatro elementos clássicos da avaliação de risco, nomeadamente as ameaças, as vulnerabilidades, os impactos na missão e nas operações do negócio e a probabilidade de ameaças na exploração de vulnerabilidades nos sistemas de informação e no ambiente físico que possam causar mal e provocar consequências adversas.

Anteriormente referido como uma metodologia com nove passos, atualmente o NIST apresenta o processo de avaliação do risco composto por quatro passos básicos. Cada passo tem associado diversos conjuntos de tarefas. Na Figura 2.15 podemos observar o processo de avaliação de risco de acordo com a metodologia NIST, assim como as tarefas específicas para o passo da realização da avaliação (passo dois).

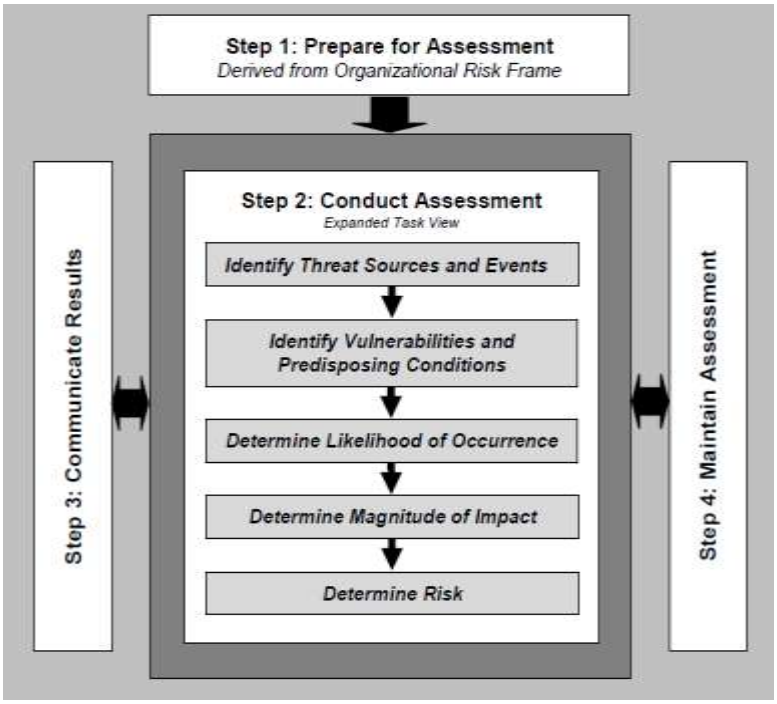

Figura 2.15 - Processo avaliação de risco (NIST, 2012)

O Passo 2 – Realizar a avaliação, consiste em produzir uma lista de riscos de segurança da informação priorizadas por nível de risco e usadas para informar as decisões de resposta ao risco. Para alcançar este objetivo, as organizações necessitam de analisar as ameaças e vulnerabilidades, impactos, probabilidades, e incertezas associadas ao processo de avaliação de risco. O passo dois contempla as seguintes tarefas:

- Identificar as fontes de ameaças relevantes para a organização;
- Identificar os incidentes que podem ser produzidos pelas fontes;
- Identificar as vulnerabilidades dentro da organização que podem ser exploradas pelas fontes de ameaças através dos incidentes específicos e das condições predisponentes que podem levar à exploração bem-sucedida;
- Determinar a probabilidade das fontes de ameaças identificadas iniciarem ataques específicos e a probabilidade dos ataques serem bem-sucedidos;
- Determinar os impactos adversos para as operações organizacionais e para os ativos, resultante da exploração de vulnerabilidades por fontes de ameaça (através de incidentes específicos); e
- Determinar os riscos de segurança da informação como combinação da probabilidade de exploração de ameaças de vulnerabilidades e o impacto

dessas explorações, incluindo incertezas associadas com as determinações de risco.

No Passo 3 – Comunicar os resultados da avaliação e partilhar a informação do risco relacionado, o objetivo é assegurar que as decisões efetuadas pela organização possuem os riscos relacionados, apropriados e necessários para informar e orientar na decisão do risco. Comunicar e partilhar informação subdivide-se nas seguintes tarefas:

- Comunicar os resultados da avaliação de risco; e
- Partilhar a informação desenvolvida durante a execução da avaliação de risco como suporte de outras atividades de gestão do risco.

O Passo 4 – Manter a avaliação consiste em manter atualizados quer o conhecimento do risco em que a organização ocorre, assim como a informação dos resultados, decisões e orientações da avaliação de risco. Incluem-se as seguintes tarefas:

- Monitorizar os fatores de risco identificados na avaliação de risco numa base contínua e perceber as alterações subsequentes desses fatores.
- Atualizar os componentes de avaliação de risco refletindo a monitorização das atividades desenvolvidas pela organização.

A metodologia *NIST Special Publications 800-30* pode ser usada por todo o tipo de organizações, públicas ou privadas, independentemente do seu tamanho. Foi desenvolvida de forma a ser consistente com os padrões ISO e flexível o suficiente para ser usado em conjunto com outras *frameworks* de avaliação de risco. De salientar que a mesma foi desenvolvida baseada nos padrões e regulações dos EUA, podendo não ser a mais adequada para organizações que seguem outro tipo de regulações.

2.3.5 *OCTAVE*

A metodologia *OCTAVE* (*Operationally Critical Threat, Asset and Vulnerability Evaluation*), foi desenvolvida pelo *Software Engineering Institute* (SEI) na *Carnegie Mellon University*, em 1999 (Caralli et al. 2007) com o intuito de enfrentar os desafios de conformidade de segurança do Departamento de Defesa (DoD) dos EUA e endereçar as disposições emanadas pelo *Health Insurance Portability and Accountability Act* (HIPAA)[9] sobre privacidade e segurança na saúde pessoal.

[9] *Health Insurance Portability and Accountability Act of* 1996 (HIPAA, Public Law 101-191) promulgado a 21 de agosto de 1996.

De acordo com o SEI *Carnegie Mellon University*, o OCTAVE é uma metodologia de identificação e avaliação dos riscos de segurança da informação que permite:

- Desenvolver critérios qualitativos de avaliação do risco que descrevam a tolerância de risco operacional da organização
- Identificar ativos que são importantes para a missão da organização
- Identificar vulnerabilidades e ameaças a esses ativos
- Determinar e avaliar as potenciais consequências para a organização caso as ameaças sejam realizadas.

Atualmente existem três metodologias distintas: OCTAVE *Method*, OCTAVE-S e o OCTAVE Allegro.

O OCTAVE *Method*, bastante completo revela-se pesado quer em termos de documentação quer em termos de processo estando direcionado sobretudo para as grandes organizações (com cerca 300 ou mais colaboradores) compostas por estruturas organizacionais por multicamadas de hierarquias e, que possuem a sua própria infraestrutura de computação. O método consiste na realização de uma série de *workshops* conduzidos por equipas de análise multidisciplinares com recurso a elementos das diferentes unidades de negócio (gestores seniores, operacionais e funcionários) e, a membros do departamento de IT da organização. Define-se como uma abordagem compreendida em três fases com oito processos (Figura 2.16). Os processos são intrínsecos às fases e são executados no decorrer das mesmas.

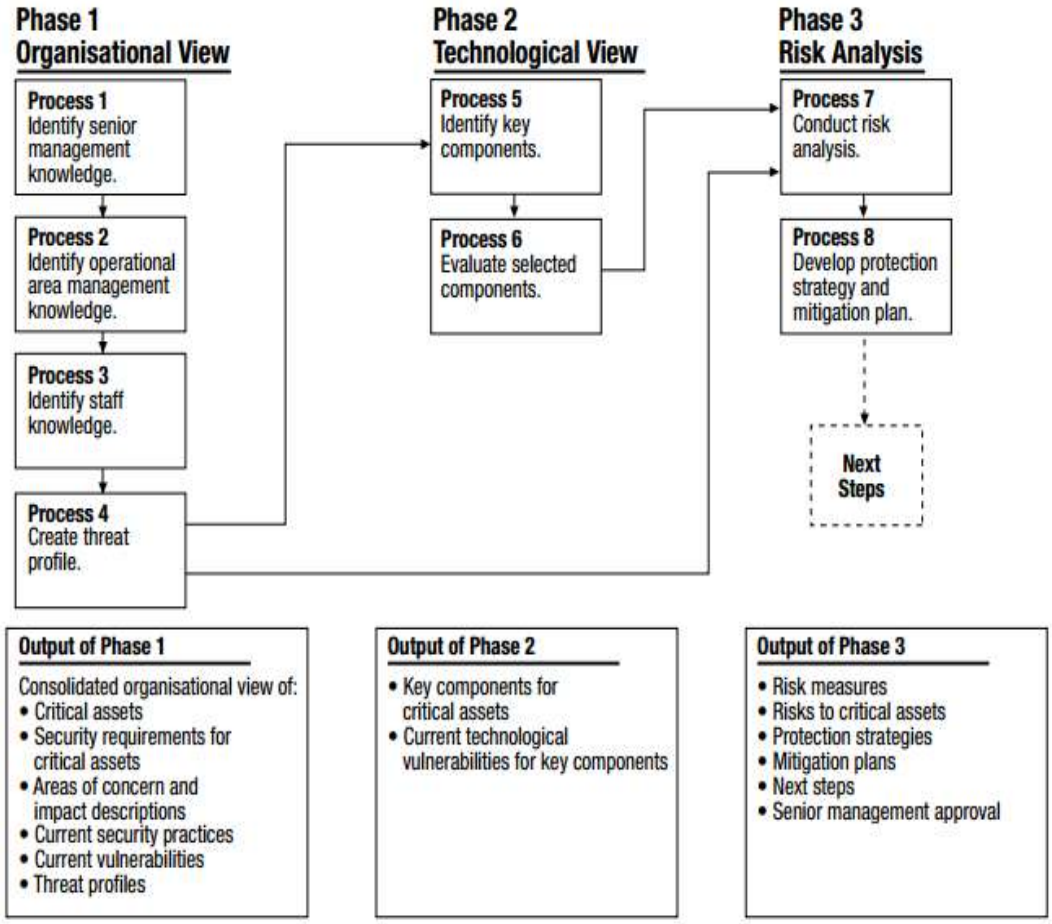

Figura 2.16 - OCTAVE Method (Panda, 2009)

As fases consistem em:

Fase 1 - Visão organizacional, onde a equipa de análise identifica e determina os ativos críticos para o sucesso da organização assim como documenta os requisitos de segurança e identifica as ameaças que possam interferir com os requisitos.

Fase 2 - Visão tecnológica, em que a equipa de análise executa uma avaliação sobre a informação da infraestrutura de forma a complementar a análise sobre ameaças realizada na fase 1 e as decisões de mitigação para a fase três.

Fase 3 - Estratégia e plano de desenvolvimento, onde a equipa de análise executa atividades de identificação dos riscos e desenvolve um plano de mitigação dos riscos para os ativos críticos.

O OCTAVE-S tem uma metodologia similar baseada nas três fases do OCTAVE Method, sendo no entanto composta por quatro processos. Está direcionado para organizações mais pequenas (com 100 ou menos colaboradores) onde o grupo multidisciplinar pode ser representado por menos pessoas (tipicamente entre três a cinco pessoas).

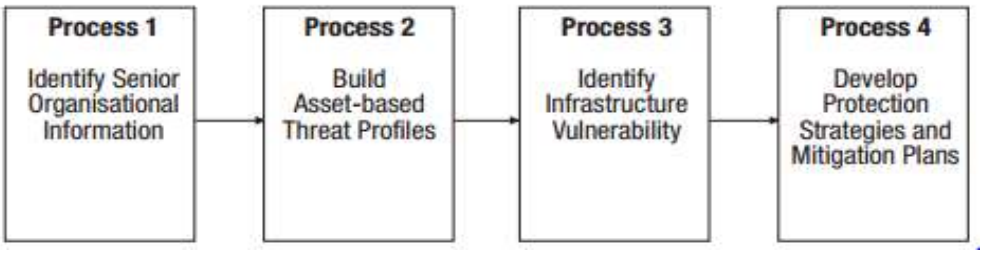

Figura 2.17 - OCTAVE-S (Panda, 2009)

No Processo 1 – Identificação da informação organizacional, são englobadas as atividades da fase um à fase três descritas no OCTAVE *Method*, assumindo-se que existe uma hierarquia organizacional plana.

O Processo 2 – Estabelecimento de "perfis de ameaças" baseado nos ativos, é baseado no processo quatro do OCTAVE *Method* e, consiste na criação de perfis tendo em conta a identificação de vulnerabilidades e ameaças correntes para cada ativo critico.

O Processo 3 – Identificação de vulnerabilidades na infraestrutura, faz o mapeamento dos processos cinco e seis do OCTAVE *Method* e, consiste na análise da infraestrutura de computação de forma a identificar componentes relacionados com o ativos críticos e a estabelecer tecnologias a vulnerabilidades.

E por último, o Processo 4 – Desenvolvimentos de estratégias de proteção e planos de mitigação, mapeia-se ao processo sete e oito do OCTAVE *Method*.

No OCTAVE-S assume-se que existe o conhecimento prático dos ativos relacionados com informações importantes, requisitos de segurança, ameaças e práticas de segurança da organização. Revela-se um método em que a documentação é menor e o processo em si é mais leve. Encontra-se mais estruturado sendo que os conceitos de segurança estão embebidos nas folhas de trabalho e de orientação permitindo lidar com o risco mesmo não havendo grande conhecimento sobre o mesmo. O OCTAVE-S permite um exame menos extenso da infraestrutura da informação e, mais adequado às pequenas organizações tendo em conta as suas limitações em termos de recursos na obtenção de ferramentas de vulnerabilidades.

O OCTAVE Allegro, consiste em oito processos organizados em quatro fases, conforme podemos observar na Figura 2.18. A abordagem OCTAVE Allegro tem como objetivo permitir uma avaliação alargada dos riscos operacionais através de resultados mais robustos sem necessidade de conhecimentos alargados de avaliação do risco. Difere das restantes abordagens ao concentrar-se principalmente em ativos de informação (como são usados, onde são guardados, transportados, processados, como

estão expostos a ameaças, vulnerabilidades e disrupções). Recorre igualmente a *workshops*, requer colaboração e baseia-se igualmente nas orientações. OCTAVE Allegro permite a avaliação de risco sem existir grande envolvimento organizacional, experiência, ou conhecimentos iniciais.

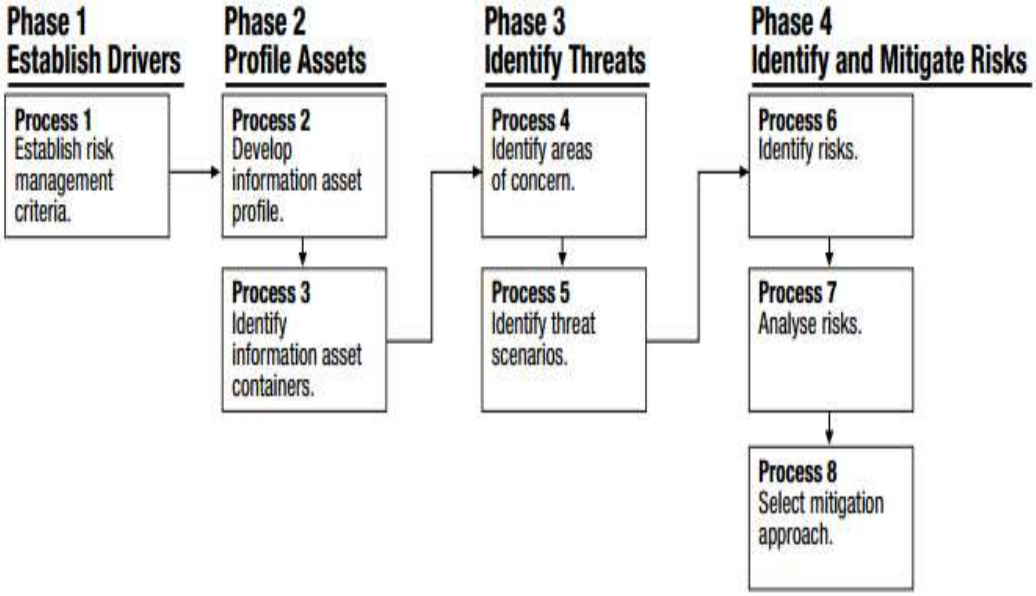

Figura 2.18 - OCTAVE Allegro (Panda, 2009)

Na primeira fase – Estabelecer orientações, são desenvolvidos critérios de medição de risco consistentes com a orientação organizacional.

Na segunda fase – Perfil dos ativos, são organizados os ativos de informação considerados críticos. O processo de organização permite estabelecer as fronteiras do ativo, identificar os requisitos de segurança, as localizações onde o ativo é guardado, transportado ou processado.

Na terceira fase – Identificar as ameaças e, com base no contexto da localização do ativo, isto é, onde é guardado, transportado ou processado, são identificadas as ameaças.

Na quarta fase – Identificar e mitigar os riscos, os riscos dos ativos de informação são identificados, analisados e são selecionadas as abordagens de mitigação.

2.4 Análise Financeira

A solução BYOD tem vindo a aumentar, sendo que numa primeira fase as organizações procuraram travar a adesão ao proibir, por exemplo, o acesso aos dados corporativos a partir dos dispositivos móveis pessoais ou atribuindo dispositivos móveis corporativos (exemplo de *laptops*) aos colaboradores (fossem colaboradores internos ou

elementos em *outsourcing*). Aos poucos, o BYOD foi conquistando o seu espaço – acesso ao correio eletrónico corporativo, acesso remoto a aplicações corporativas a partir de dispositivos pessoais. Apesar desse aumento, a maioria das organizações não avaliou o impacto financeiro do novo modelo de ICT, havendo ainda dúvidas quanto aos custos e benefícios de uma solução BYOD. Assim, o grande desafio é tirar partido da solução BYOD. Para que a adesão tenha sucesso importa perceber quais os custos e benefícios com a introdução de uma solução BYOD na organização, quais os investimentos necessários e o ponto de retorno do investimento. Os dispositivos usados no acesso aos dados corporativos deixou de ser somente uma preocupação da área de ICT, mas passa também por envolver os gestores de topo e o parecer da área financeira.

Este capítulo pretende fazer uma breve introdução de algumas análises financeiras que podem ser úteis num cenário BYOD e lançar as bases para a construção de um *business case* que permita justificar e apoiar a implementação de uma solução BYOD.

> *"The cost and benefits of security should be carefully examined in both monetary and non-monetary terms to ensure that the cost of controls does not exceed expect benefits."*[10]

2.4.1 Análise Custo-benefício

A Análise Custo-Benefício (*Cost-Benefit Analisys – CBA*) consiste em comparar o custo de um sistema com o benefício em ter esse sistema. São somados os potenciais benefícios de uma determinada situação ou ação relacionada com o negócio e de seguida são subtraídos os custos associados com a tomada dessa decisão. Sendo assim a fórmula básica da Análise Custo-Benefício consiste em subtrair aos benefícios os custos: $CBA = Benefícios - Custos$

A Análise Custo-Benefício funciona como um meio que permite avaliar todos os custos e a potencial receita (antecipação dos benefícios) que pode ser gerada caso se opte por um determinado projeto. O resultado da análise vai determinar se o projeto é viável financeiramente ou se deve ser abandonado.

Apesar de parecer relativamente simples, a aplicação da Análise Custo-Benefício pode ser complexa, em parte devido ao número de variáveis introduzidas. Outro especto a considerar relaciona-se com a necessidade de estimar os custos diretos e indiretos

[10] Citação "*Generally Accepted Principles and Practices for Securing Information Technology Systems"* (NIST, 1995)

assim como os benefícios tangíveis e intangíveis tendo por base a mesma medida (de preferência de unidade monetária).

No caso BYOD, os benefícios intangíveis podem ser, por exemplo, a rapidez / prontidão de resposta e, ou o aumento da satisfação / motivação dos colaboradores que podem traduzir-se em aumento de produtividade. Sendo assim, na relação custo-benefício importa detalhar fatores qualitativos de forma quantitativa para que os resultados sejam fáceis de compreender e se tornem tangíveis. Em termos de custos, a análise pode ser feita considerando o investimento em equipamento móvel e, ou a partilha ou, mesmo a transferência dessa despesa para os colaboradores, tendo em conta que alguns colaboradores estão dispostos a investir em dispositivos topo de gama ou de última geração.

Ainda para a solução BYOD, importa considerar custos corporativos em termos da necessidade de desenvolvimento de compatibilidades das aplicações corporativas com os dispositivos móveis, formação e suporte técnico entre as aplicações e os dispositivos pessoais dos colaboradores. Tratando-se de equipamentos há que considerar também a questão das amortizações, caso a compra seja da responsabilidade da organização. O ideal é documentar todos os fatores a considerar. Com recurso à relação benefício-custo (B*enefit-to-Cost Ratio - BCR)* é possível determinar a viabilidade do projeto tendo em conta um período de tempo e as respetivas variações.

Como desvantagens da Análise Custo-Benefício são apontadas dificuldades na definição precisa dos custos e benefícios tendo em conta o número de variáveis possíveis. Outra questão prende-se com a necessidade em quantificar os impactos não-monetários, tendo em conta que a CBA não considera custos e benefícios intangíveis.

2.4.2 Análise Break-Even

A análise *break-even* em termos gerais permite determinar o momento em que a receita recebida igualiza os custos associados. Qualquer projeto implica investimento inicial (custo). No entanto, há que considerar quando é expectável que as receitas atingem ou superem o valor do investimento. A análise *break-even* calcula a margem de segurança, ou seja, o montante em que as receitas excedem o ponto de equilíbrio (*break-even point*). Tendo em conta essa margem, as receitas podem descer representando igualmente lucro desde que se mantenham acima do ponto de equilíbrio anteriormente definido. A análise *break-even* pode ser efetuada considerando diferentes cenários.

Em termos de solução BYOD e, considerando a existência de múltiplas alternativas, a análise que demonstrar o menor *break-even point* será a solução ideal, uma vez que representa atingir o ponto de equilíbrio mais cedo.

Em termos de desvantagens, a análise *break-even* não considera possíveis variações de mercado, e reporta-se à estimativa de lucros e custos na altura da análise. Sendo assim e, caso haja alterações, o ponto de equilíbrio estimado pode apresentar incorreções. Por outro lado, em novos serviços (caso da solução BYOD), a análise *break-even* pode revelar alguma falta de precisão na estimativa das variáveis, uma vez que não existe um historial dos valores de referência que permitam suportar a análise de *break-even*.

2.4.3 Retorno sobre Investimento *(ROI)*

O Retorno Sobre Investimento, ou *Return on Investment (ROI)*, consiste numa medida de desempenho usada para avaliar a eficiência de um investimento ou comparar a eficácia de diferentes investimentos. Mede a quantidade de retorno de um investimento em relação ao seu custo. Consiste em dividir o benefício (ou retorno) de um investimento pelo custo do investimento sendo o resultado, expresso em percentagem ou rácio: $ROI = \frac{(Beneficio - Custo)}{Custo}$

Quanto maior o ROI, maior o retorno obtido. O ROI é uma medida simples de calcular e de interpretar e pode ser aplicada a uma variedade de investimentos. Sendo expressa em percentagem facilmente permite comparar qual o investimento preferível em relação a outro. Existem no entanto diferentes métodos de cálculo do ROI, sendo os mais usuais: *Net Present Value* (NPV) e a *Internal Rate of Return* (IRR).

Net Present Value (NPV)

O *Net Present Value* (NPV) (Investopedia, 2015b) ou o Valor Presente Líquido (VPL) também designado por Valor Atual Liquido (VAL) consiste na diferença entre o valor presente dos fluxos de caixa (*cash inflows*) e o valor presente de saídas de caixa (*cash outflows*). A fórmula usada é: $NPV = C_0 + \sum_{t=1}^{n} \frac{B_t - C_t}{(1+r)^t}$

Sendo que:

$B_t - C_t$ representa as entradas líquidas durante o período t ;

C_0 representa os custos totais do investimento inicial

r representa a taxa de desconto e

t representa o número de períodos de tempo.

Um NPV positivo indica que os ganhos projetados gerados por um projeto ou investimento excedem os custos previstos, pelo que o investimento é considerado rentável. No caso de um NPV negativo prevê-se que o investimento resulte em perda líquida, não sendo aconselhável o investimento. A taxa de desconto (r) permite medir o valor de caixa futuro e assim avaliar se o investimento hoje é compensatório em relação a ganhos futuros, tendo em conta que o valor monetário do presente tem mais valor que a mesma quantidade do mesmo valor monetário do futuro (influenciado por fatores como *time value money* e a inflação).

Internal Rate of Return (IRR)

A *internal rate of return* (IRR) (Investopedia, 2015a) ou a Taxa Interna de Rendibilidade (TIR), é a taxa de desconto que faz com que o NPV de todos os fluxos de caixa de um projeto em particular tende para zero.

Se a IRR> TA (taxa de atualização) implica que o NPV> 0, então o projeto consegue gerar uma taxa de rendibilidade superior ao custo de oportunidade do capital, pelo que estamos perante um projeto economicamente viável; se a IRR <TA implica que o NPV <0, então o projeto não consegue gerar uma taxa de rendibilidade superior ao custo de oportunidade do capital, pelo que estamos perante um projeto economicamente inviável. O cálculo do IRR é efetuado com base na fórmula NPV, sendo os conceitos os mesmos: $C_0 = \sum_{t=1}^{n} \frac{B_t - C_t}{(1+IRR)^t}$

No entanto, assume-se que o NPV é igual a zero e resolve-se a taxa de desconto (r), que será a IRR. A IRR não pode ser calculada analiticamente, sendo por meio de tentativa e erro através de *software* (exemplo da fórmula IRR ou TIR em português, disponível na folha de cálculo Microsoft Excel). A IRR fornece informação útil em particular quando existem constrangimentos em termos de orçamento ou quando existe incertezas quanto à taxa de desconto.

Com a IRR pode-se comparar vários projetos, sendo que, e assumindo-se que os custos de investimento são iguais entre os projetos, o projeto com IRR superior será provavelmente o melhor e deve ser executado em primeiro lugar.

No caso da solução BYOD e para calcular o ROI é conveniente envolver as áreas de ICT e financeira. Existindo diversos fatores, importa igualmente distinguir os que devem ser considerados e os que podem ou devem ser ignorados.

2.5 Resumo

A escolha de uma metodologia de gestão e avaliação de risco não é linear e depende de uma série de circunstâncias, pelo que respondendo à questão: Q1. Qual a metodologia de Avaliação e Gestão de Risco a seguir?, as organizações devem previamente avaliar os seus objetivos e escolher a metodologia de risco que melhor se adaptem às suas necessidades.

Como podemos observar, as metodologias de risco diferem sobretudo na descrição e nos detalhes associados aos passos necessários para a realização da avaliação de risco, sendo algumas mais complexas do que outras, no entanto apresentam estruturas similares, nomeadamente na necessidade de existir processos que vão permitir aplicar uma metodologia de gestão e avaliação de risco que possibilite:

i) Identificar os ativos e as partes interessadas (*stakeholders*);
ii) Compreender os requisitos de segurança;
iii) Identificar as ameaças/vulnerabilidades;
iv) Identificar e avaliar a eficácia dos controlos e,
v) Calcular o risco baseado quer no risco inerente, quer no compromisso e, ou na probabilidade da ameaça vir a concretizar-se.

Uma metodologia de risco não responde a todas as necessidades havendo vantagens e desvantagens entre elas, pelo que, as organizações devem optar por complementarem a sua avaliação de risco recorrendo, se for o caso, a mais do que uma metodologia.

As metodologias OCTAVE, NIST e FAIR focam-se sobretudo na questão da avaliação do risco, e as metodologias COBIT 5 e ISO 27005:2011 centram-se mais na questão da gestão do risco, no entanto o COBIT 5 abrange toda a componente ICT (desde o desenvolvimento, continuidade de negócio e outro tipo de riscos operacionais de ICT), enquanto a ISO 27005:2011 concentra-se exclusivamente em segurança. Por outro lado, as metodologias ISO 27005:2011 e NIST apesar de diferentes seguem uma estrutura similar e funcionam como referências na definição de uma metodologia de avaliação de risco. Uma das vantagens da metodologia OCTAVE relaciona-se com a disponibilização de formulários que permitem documentar cada passo do processo, podendo os mesmos serem alterados e customizados pelas organizações. No Anexo A - Resumo Metodologias de Análise e Avaliação de Risco, são destacados os principais aspetos das metodologias analisadas.

No que concerne à análise financeira, foram apresentados alguns indicadores financeiros de base que as organizações podem usar, respondendo assim à questão: Q2. Que indicadores financeiros devem ser considerados que demonstrem a viabilidade da solução BYOD?

As organizações necessitam de se munirem de um variado conjunto de estratégias que avaliem o valor e o impacto ao incorporar despesas e atividades relacionadas com a implementação de uma solução BYOD. O custo da solução BYOD varia de organização para organização e vai depender de diversos fatores, sendo aconselhável o recurso a *business case* financeiro.

Uma vantagem imediata em termos de custos pode ser a transferência dos gastos relacionados com as comunicações e com os equipamentos, que podem ser transferidos da organização para o colaborador, tendo em conta a vontade dos colaboradores em terem um só dispositivo móvel e, ou de estarem dispostos a título particular em adquirirem os dispositivos móveis de última geração. Por sua vez, os ganhos em termos de produtividade vão depender sobretudo da cultura da organização e da disposição dos colaboradores em trabalharem tendo por base o conceito BYOD (*anytime / anywhere*).

Por outro lado, se a solução de BYOD pode significar poupanças em termos de equipamento e telecomunicações e ganhos em termos de produtividade, é necessário perceber os custos adicionais, nomeadamente da infraestrutura e, ou do suporte à solução.

A análise financeira deve comportar diversas alternativas e considerar os vários cenários. Deve igualmente e, sempre que possível, transformar todos os valores na mesma medida unitária e quantificar os benefícios intangíveis que podem ter influência no projeto. Vai permitir seguir a solução BYOD que se apresente mais favorável à organização. Dependente do que se pretende podem ser usadas diferentes análises financeiras conforme descrito. Para que a análise seja eficaz é necessário definir o que se pretende analisar, estabelecer a relação entre os fatores e quantificar na mesma medida todas as variáveis pertinentes para a análise, quer sejam quantitativas, quer sejam qualitativas. É necessário ter igualmente presente o tempo de execução dos projetos e que o retorno não é imediato, sendo necessário projetar taxas de descontos, inflação e o valor do dinheiro no tempo.

Capítulo 3

Análise a soluções BYOD

Neste capítulo, para além da revisão da literatura científica, são abordadas as questões relacionadas com a análise dos riscos presentes na solução BYOD, dos custos e benefícios da mesma, dos requisitos legais e da constituição de políticas de segurança BYOD.

Cada vez é mais usual assistir à utilização dos dispositivos pessoais para questões relacionadas com o trabalho. É inegável a capacidade estabelecida com os dispositivos móveis, nomeadamente o facto de se deixar estar confinado a um edifício ou a um dispositivo. A possibilidade de responder em qualquer lugar, em qualquer altura e a possibilidade de escolha entre uma gama de dispositivos e de aplicações torna a solução BYOD bastante atrativa, quer para os colaboradores, quer para os gestores de negócio.

Considerando a utilização de dispositivos pessoais no local de trabalho, as empresas necessitam de adotar uma visão do BYOD que proteja a rede e os dados, independentemente da forma de acesso à informação.

Nesse sentido os departamentos de ICT assumem um papel importante e necessitam de antecipar e prepararem-se para as perturbações que acontecerão num ambiente BYOD. Não significa que passem a aceitar riscos elevados mas também não significa que o departamento de segurança constitua uma barreira à transformação emergente do negócio.

It's not a question of if. It's not even a question of when. It's a question of, will you be ready?[11]

[11] Citação em *Bring Your Own Devices (BYOD) Survival Guide (*Keyes, 2013)

3.1 Revisão de Literatura

Nunoo (2013) apresenta um estudo com base numa perspetiva sociotécnica e identifica uma série de ameaças, riscos e vulnerabilidades que podem ser associados à utilização de dispositivos móveis (especificamente *smartphones*) quando a segurança não é uma das prioridades do utilizador ou de quem lhes atribui o dispositivo (ou seja, da organização). O estudo revela que os colaboradores apesar de quererem salvaguardar a sua privacidade não pretendem ser sobrecarregados com as questões de segurança considerando que as definições e configurações de segurança dos *smartphones* são da responsabilidade das organizações, sobretudo se a organização é a proprietária do dispositivo. A maioria dos proprietários de *smartphones* desconhecem os requisitos de segurança aplicáveis, nomeadamente a existência de antivírus para *smartphones*, mecanismos de *wipe* remoto, mecanismos de criptação, os riscos que as aplicações podem incluir e/ou a necessidade de proteger o acesso às aplicações corporativas com password ou PIN. O autor conclui que é vital estabelecer uma política de segurança eficaz sem ser no entanto bloqueadora. A segurança deve ser transmitida de cima para baixo (*top-down*) e não de baixo para cima (*bottom-up*) funcionando dessa forma como um modelo a seguir na organização. A solução passa por definir uma política e procedimentos, na educação e formação dos colaboradores e na utilização da tecnologia e de controlos eficazes. As organizações devem fazer a sua avaliação de risco e avaliar especificamente os riscos face aos potenciais benefícios.

Lydon (2014) elabora uma revisão sistemática da literatura relacionada com o BYOD em SME's (*Small or Medium Enterprises*). Neste trabalho são apresentados os benefícios do BYOD nas organizações, nomeadamente o aumento da produtividade e eficiência dos colaboradores. São igualmente apresentados os riscos inerentes à adesão a uma solução BYOD e, que podem ser verificados com maior detalhe neste capítulo, na secção de Gestão do Risco BYOD. Lydon refere igualmente a importância na definição de uma política de segurança para dispositivos móveis compreensiva que permita clarificar as questões de uso aceitável para os dispositivos móveis consistente com outras políticas de segurança e privacidade da organização. A política de segurança para dispositivos móveis vai permitir estabelecer limites para quem pretenda utilizar os seus próprios dispositivos no local de trabalho. No que se refere às SME's, são apontados as dificuldades que as organizações enfrentam na implementação de mecanismos de proteção de dados e de segurança ICT. Estas empresas reservam uma ínfima parte do

orçamento para as questões da segurança e, geralmente, só tomam consciência dessa necessidade quando são afetadas (ou seja, quando sofrem algum tipo de ataque que comprometem os seus dados comerciais). Este autor, sugere o recurso a soluções MDM (*Mobile Device Management*), como das soluções mais abrangentes e completas na implementação de segurança BYOD, no entanto face ao custo enumera os controlos mínimos baseados nas recomendações pelo *National Institute of Standards and Technology* (NIST) e o *Federal Bureau of Investigation* (FBI) nomeadamente, assegurar que: a) não é permitido *jail-broken* (manutenção do sistema operativo do fornecedor sem alterações) nos dispositivos; b) o dispositivo é bloqueado após período de inatividade; c) é instalado software de antivírus; d) são efetuadas atualizações periódica dos sistemas/aplicações; e) existem mecanismos de proteção (*passwords*, *passhphrases*, *pin*, etc); f) os dados corporativos nos dispositivos são salvaguardados (backup); g) é possível efetuar limpeza remota (*remote wipe*); h) as aplicações só são instalados a partir de lojas de *apps* oficiais (exemplo Google Play, Windows Store, iTunes, etc); i) as comunicações por Wi-Fi são feitas através de redes seguras (exemplo por VPNs - *Virtual Private Networ*); j) existe uma política de segurança BYOD; g) os colaboradores estão cientes das suas responsabilidades e dos riscos associados quando utilizam os dispositivos móveis. Lydon sugere que sejam seguidas as recomendações emanadas pelas normas ISO/IEC 27000, mais concretamente pela ISO 27001:2013 (ISO/IEC, 2013). Refere ainda a importância de instruir os colaboradores nas adoção de políticas de segurança, sendo esse um dos fatores mais críticos que as organizações enfrentam, ou seja, dos colaboradores não seguirem os procedimentos de segurança definidos.

Weber (2014) com base na revisão de literatura identifica alguns dos potenciais riscos da solução BYOD (descritos com maior detalhe neste capítulo, na secção Gestão do Risco BYOD) e classifica-os em: riscos de preocupações estratégicas incrementais e preocupações operacionais. Recorrendo ao COBIT 5 apresenta uma *framework* onde analisa os riscos incrementais com o objetivo de reduzi-los para um nível de risco aceitável. Já em 2013, a NIST tinha publicado um documento relativo às orientações de gestão dos dispositivos móveis nas organizações (NIST, 2013).

No trabalho Agudelo et al. (2015) salienta-se o papel que o comportamento dos colaboradores que recorrem aos dispositivos móveis desempenham e que podem levar ao risco de fuga ou perda de conhecimento (*knowledge leakage*), um dos principais riscos da solução BYOD. Foram definidos dois tipos de comportamentos internos: acidental e malicioso, sendo que o comportamento acidental, para além de ser mais

frequente, quando exercido internamente tem um potencial de risco superior aos ataques internos maliciosos. Em relação ao conhecimento, foram identificados dois tipos: o conhecimento presente nos colaboradores (relacionado com a retenção de valores), que não foi abordado e, o conhecimento que é codificado em artefactos como por exemplo documentos, processos ou procedimentos, sendo sobre este tipo de conhecimento, produzido em ambiente tecnológico, que foi analisado o risco de fuga. Com recurso a meios tecnológicos e com base nos dispositivos móveis os colaboradores podem aceder aos dados corporativos fora da organização. O estudo indica igualmente as diferenças entre o conceito de dispositivos móveis pessoais e dispositivos corporativos, sendo que os dispositivos móveis pessoais, sendo do colaborador, implicam maior probabilidade de modificação em relação aos dispositivos móveis corporativos (apesar destes também poderem ser igualmente customizados pelo colaborador, são supostamente controlados pela organização).

Outro aspeto focado relaciona-se com o contexto - ambiental, organizacional e social, que rodeia os colaboradores e que influencia o comportamento dos indivíduos, sendo o contexto social o que maior influencia o risco de perda de conhecimento. A aplicação de políticas de segurança são mais difíceis de implementar quando o dispositivo é do colaborador e quando o mesmo utiliza-o fora do perímetro da organização, estando condicionado à pressão (como seja o de executar o trabalho pendente, uma resposta de email urgente, ou outra atividade de caráter urgente), ao ambiente social (espaços públicos como aeroporto, estação de comboios, etc.) e tecnológico (existência de redes públicas não seguras) que possibilitam que inadvertidamente o colaborador descure as regras de segurança. O estudo conclui que apesar de não ser possível prever os riscos de fuga de conhecimento que podem advir do comportamento do colaborador, as organizações devem fazer um esforço para perceber os fatores que influenciam os "colaboradores móveis" e, nesse sentido estabelecer níveis de comportamento de segurança compatíveis, controlos preventivos técnicos e estabelecer políticas de segurança, e programas de sensibilização, formação e educação de segurança para compensar as influências que os fatores externos exercem.

Arregui (2015) considera que apesar do aumento das preocupações da segurança de informação, as organizações não conseguem travar a tendência do BYOD. Assim considera que o desafio das organizações em estabelecer práticas de segurança nos dispositivos de que não são proprietários passa por entender e agrupar os riscos mais significativos em três grandes áreas: i) comportamentos dos utilizadores, ii)

procedimentos de conetividade e iii) práticas de gestão. O estudo revela que o recurso a ferramentas MDM permite mitigar de forma adequada os riscos do BYOD. Revela igualmente que as organizações necessitam de melhorar as boas práticas relacionadas com os procedimentos de ligações. Recomenda que sejam desenvolvidos procedimentos de segurança da informação eficientes de forma a mitigar os riscos do BYOD quando os dispositivos são ligados em redes não corporativas. O autor alerta igualmente para o facto das organizações terem diferentes prioridades e objetivos em relação à segurança da informação pelo que o desenvolvimento de procedimentos de segurança deve ser conduzido tendo em conta essa realidade, assim como deve considerar os riscos da segurança de informação dentro do sector da indústria em que se enquadra.

Na Tabela 3.1 é apresentado um quadro resumo da revisão da literatura científica.

Autor	Âmbito	Ideia principal	Proposta	Conclusão
Nunoo (2013)	Perspetiva sociotécnica (*smartphones*)	• Desresponsabilização pelas questões de segurança •Desconhecimento dos requisitos de segurança aplicáveis	• Antivírus • *Wipe* remoto • Mecanismos de criptação • Password ou PIN	• Definir política de segurança • Investir na educação e formação dos colaboradores • Utilizar tecnologia e controlos eficazes • Avaliar os riscos e potenciais benefícios
Lydon (2014)	Revisão literatura do BYOD em SME's	• Aumento da produtividade e eficiência dos colaboradores • Riscos	• Recurso a soluções MDM ou • Controlos mínimos baseados nas recomendações do NIST e do FBI	• Definir política de segurança • Implementar mecanismos de proteção de dados e de segurança ICT • Instruir os colaboradores sobre responsabilidades e riscos
Weber (2014)	Revisão de literatura	Dois tipos de preocupações: • estratégicas incrementais • operacionais	• *Framework* baseada no COBIT 5	• Reduzir os riscos incrementais para níveis de risco aceitável
Agudelo et al. (2015)	Comportamento Conhecimento Contexto	• Risco de fuga ou perda de conhecimento • Comportamentos de risco • Informação em dispositivos não-controlados • Diferenças entre dispositivos pessoais e dispositivos corporativos • Contexto ambiental, organizacional e social	• Perceber os fatores que influenciam os colaboradores • Estabelecer níveis de comportamento de segurança • Compensar as influências que os fatores externos exercem.	• Definir controlos preventivos técnicos • Estabelecer uma política de segurança • Estabelecer programas de sensibilização, formação e educação
Arregui (2015)	Práticas de segurança	Riscos agrupados em: • Comportamento dos utilizadores • Procedimentos de conetividade • Práticas de gestão	• Recurso a ferramentas MDM • Melhorar as boas práticas relacionadas com conetividades • Procedimentos de segurança adequados	• Desenvolver procedimentos de segurança da informação eficientes, baseados nas prioridades e objetivos da organização • Considerar os riscos da segurança de informação dentro do sector da indústria da organização

Tabela 3.1 - Resumo revisão da literatura científica

3.1.1 Requisitos Legais BYOD

Com a adoção de uma solução BYOD, os dados corporativos deixam de estar circunscritos aos sistemas proprietários da organização para estarem residentes nos dispositivos pessoais móveis dos colaboradores. As informações de dados financeiros, de clientes, de projetos, etc., passam a estar acessíveis através de *smartphones*, *tablets* ou *laptops* dos colaboradores internos ou externos, existindo por parte da organização a responsabilidade e a obrigação de salvaguardar igualmente esses dados, independentemente do dispositivo de acesso ou armazenamento.

De acordo com Costa (2015), a legislação portuguesa prevê que as organizações providenciem aos colaboradores os mecanismos necessários para a execução das suas atividades, pelo que a adesão a soluções BYOD deve ser encarada uma ação voluntária, no caso do colaborador utilizar os seus dispositivos pessoais.

Não sendo o objetivo deste trabalho efetuar um levantamento exaustivo da legislação portuguesa, as organizações devem no entanto considerar, em termos de cenários corporativos na implementação de uma solução BYOD, os seguintes aspetos:

i) As obrigações com a proteção dos dados sensíveis corporativos, (Costa, 2015; Mavretich, 2012) incluindo dados de negócio, dados confidenciais, ou seja, restritos à organização e dados privados como por exemplo informação de clientes e/ou de colaboradores;

ii) As possíveis quebras de segurança (Costa, 2015) que podem originar processos legais com consequências nefastas em termos financeiras ou em termos de reputação e imagem. Em caso quebra de segurança, o colaborador deve sentir-se "à vontade" para participar a situação. Sendo um dispositivo pessoal, e caso não haja essa relação de confiança, a quebra de segurança pode não ser reportada por desconhecimento ou por medo de represálias (Mavretich, 2012);

iii) As questões de regulação e legislação aplicável a determinados setores (Costa, 2015; Mavretich, 2012; Gilmore et al., 2013) como por exemplo, aos serviços de comunicações eletrónicas (obrigados a comunicar às autoridades qualquer violação de dados, conforme Lei n.º 46/2012, de 29 de agosto), ou relacionados com informação médica (cujos dados não podem serem monitorizados, conforme Lei n.º 67/98, de 26 de outubro);

iv) Os requisitos legais aplicáveis aos territórios (Costa, 2015; Gilmore et al., 2013) sendo aconselhável efetuar um levantamento prévio da legislação para

os casos onde os colaboradores tenham que aceder com os seus dispositivos a conteúdos corporativos.

Em termos laborais é necessário considerar cenários como:

i) A potencial intrusão das organizações nos dados pessoais dos colaboradores, protegidos pela legislação portuguesa conforme número 1 do artigo 22º, do Código do Trabalho e Lei n.º 46/2012, de 29 de agosto, não podendo ser acedidos pela entidade patronal sem consentimento expresso do colaborador (Costa, 2015; Mavretich, 2012);

ii) O licenciamento de *software* e penalidades (Costa, 2015; Gilmore et al., 2013) caso se verifique por exemplo a utilização de *software* de uso privado (exemplos, *home edition* ou *student edition*), geralmente instalado nos dispositivos pessoais em vez de *software* para fins comerciais ou profissionais (exemplo do número 1 e 2 do artigo 6º da Lei 109/2009 de 15 de setembro); e

iii) Os potenciais riscos laborais, nomeadamente pelo pagamento de horas complementares, direitos de *copyright* de informação produzida em dispositivos pessoais fora do horário de trabalho, e despesas extras relativas a comunicações (Costa, 2015).

A capacidade por parte das organizações em provar que foram tomadas as medidas razoáveis para evitar a perda ou a eliminação de dados pode atenuar penalidades caso o assunto seja levado a tribunal (Gilmore et al., 2013). Importa referir que não existe uma lista concreta de medidas razoáveis que devem ser tomadas, sendo que dependem sobretudo:

i) Do setor ao qual a organização está afeta (seja o setor primário, que compreende as atividades ligadas à natureza, como sejam a agricultura, a silvicultura, as pescas, a pecuária, a caça ou as indústrias extrativas; o sector secundário, no qual são englobadas as atividades industriais transformadoras, a construção, a produção de energia; ou o sector terciário (ou dos serviços), que engloba o comércio, o turismo, os transportes e as atividades financeiras);

ii) Do valor da informação;

iii) Das consequências com a eventual perda de dados;

iv) Do nível de investimento com as medidas de prevenção; e,

v) De como é que as outras organizações procedem em situações semelhantes.

Outro aspeto a considerar e sendo o fenómeno BYOD recente, é que não existe muita informação das melhores práticas a seguir, pelo que devem ser aplicadas práticas

de segurança e expectativas normais de precauções de segurança razoáveis, sendo que o "razoável" altera rapidamente, devendo haver sempre um acompanhamento das mudanças.

Um dos primeiros passos para a implementação da solução BYOD é a definição de uma política de segurança concisa que considere os dispositivos móveis e o BYOD de forma explícita e clara para todos os colaboradores (Mavretich, 2012; Gilmore et al., 2013) devendo existir a aceitação por escrito da solução BYOD por parte do colaborador (Costa, 2015). De referir que em caso de quebra de segurança, caso se verifique o incumprimento da política por parte da organização, essa questão pode ser aproveitada no apuramento das responsabilidades (InfoLawGroup, 2012).

Outra procedimento é atualizar e rever periodicamente a política de forma a refletir as alterações e melhorias definidas pela organização, assim como outras alterações de negócio ou de risco (Costa, 2015).

A organização deve igualmente considerar ações de comunicação e sensibilização junto dos colaboradores (Lydon, 2014; Agudelo et al., 2015). Dependendo da capacidade de assimilação dos colaboradores e sobretudo da cultura da empresa, deve ser estipulado o tipo de formação mais adequada. Se existir uma cultura de segurança na organização (Nunoo, 2013), pode ser suficiente realizar sessões de formação do tipo *e-learning* já com algum nível de maturidade. Caso contrário poderá ser necessário, numa primeira fase, instituir sessões mais formais e presenciais junto dos colaboradores. Face à constante evolução tecnológica deve ser considerado igualmente sessões de atualização periódicas (por exemplo, uma vez por ano).

No caso de contratação de serviços externos deve ser igualmente disponibilizada a política de segurança junto dos parceiros, possibilitando que os mesmos tomem conhecimento das medidas de segurança e adotem os mecanismos necessários que permitam cumprirem igualmente com os requisitos.

Na Tabela 3.2 é apresentado um resumo da revisão da literatura em relação aos requisitos legais que devem ser considerados na implementação de uma solução BYOD.

Autor	Perspetiva	Particularidade	Legislação
Costa (2015)	• As organização devem providenciar aos colaboradores os mecanismos necessários para a execução das suas atividades	• O BYOD deve ser encarada uma ação voluntária • Requer a aceitação por escrito da solução BYOD por parte do colaborador	
Costa (2015) Mavretich (2012)	• Obrigações com a proteção dos dados sensíveis corporativos		
Costa (2015) Mavretich (2012)	• Comunicação de possíveis quebras de segurança		
Costa (2015) Mavretich (2012) Gilmore et al (2013)	• Regulação e legislação aplicável a determinados setores	• Serviços de comunicações eletrónicas - obrigados a comunicar às autoridades qualquer violação de dados	• Lei n.º 46/2012, de 29 de agosto
		• Serviços de informação médica - cujos dados não podem serem monitorizados	• Lei n.º 67/98, de 26 de outubro
Costa (2015) Gilmore et al. (2013)	• Requisitos legais aplicáveis aos territórios	• Efetuar um levantamento prévio da legislação	
Costa (2015) Mavretich (2012)	• Potencial intrusão nos dados pessoais dos colaboradores por parte das organizações	• Os dados pessoais não podem ser acedidos pela entidade patronal sem consentimento expresso do colaborador	• Número 1 do artigo 22º, do Código do Trabalho • Lei n.º 46/2012, de 29 de agosto
Costa (2015) Gilmore et al. (2013)	• Licenciamento de *software* e penalidades	• Utilização de software de uso privado (*home edition* ou *student edition*) em vez de *software* para fins comerciais ou profissionais	• Número 1 e 2 do artigo 6º da Lei 109/2009 de 15 de setembro
Costa (2015)	• Potenciais riscos laborais	• Pagamento de horas complementares, direitos de *copyright* de informação produzida em dispositivos pessoais fora do horário de trabalho, e despesas extras relativas a comunicações	• Código do Trabalho

Tabela 3.2 - Resumo requisitos legais BYOD

3.1.2 Riscos BYOD

Qual o risco que o BYOD representa para a organização? Em primeiro lugar as organizações devem definir o significado do que consideram como "risco". De seguida devem estabelecer: i) os ativos em risco, ii) as possíveis ameaças, iii) os vetores de ataques e, iv) os controlos que vão permitir minimizar os impactos, e desse modo direcionar as ameaças para níveis de risco aceitáveis. Após a definição de risco devem ser estabelecidos os vários cenários de risco. A definição do modelo ou cenário de risco baseia-se em condições básicas e assunções, sendo vital identificar os pressupostos

chave para os cenários em concreto. Os cenários de risco podem ser redefinidos sempre que a organização assim o entenda.

Os ativos em risco são principalmente os ativos que a organização pretende proteger e, que no seu entender são críticos para a organização. Atualmente a "informação" é um dos ativos mais críticos de qualquer organização. Em traços gerais pode-se considerar como ativo a proteger, os dados, por exemplo: i) de clientes, ii) corporativos, iii) financeiros, iv) e, ou outros. Para cada risco devem ser quantificados valores baseados sobretudo nas experiências do passado (como por exemplo frequência de ocorrências idênticas ou similares, impactos adjacentes e condições de controlo).

Em termos de análise de ameaças, e com recurso a um modelo de ameaças é possível identificar requisitos de segurança e desenvolver uma solução para os dispositivos móveis que incorpore os controlos necessários para responder aos objetivos de segurança. Sendo assim, o modelo de ameaças deve incorporar numa primeira fase os recursos de interesse, as ameaças viáveis, as vulnerabilidades e os controlos relacionados com os recursos. De seguida deve ser quantificada a verosimilhança de sucesso dos ataques e os respetivos impactos, sendo o valor da verosimilhança associado à estimativa de probabilidade, pelo que o termo probabilidade será usado para representar essa estimativa.

Por último, deve ser analisada a informação de forma a determinar se devem ser melhorados ou adicionados novos controlos de segurança.

Numa solução BYOD, e em termos de modelo de ameaças e adaptando as orientações emanadas por NIST (2013), no que se refere à gestão dos dispositivos móveis nas organizações podem ser estabelecidas quatro áreas: i) segurança física, ii) dispositivos móveis, iii) redes e, iv) aplicações.

Considerando a área da i) segurança física identifica-se que o roubo ou a perda de dispositivos móveis é das maiores ameaças de segurança que as organizações enfrentam. A perda de um dispositivo móvel, com dados corporativos confidenciais representa o risco de comprometimento dos dados principalmente se não foram adotadas medidas de proteção como, por exemplo, autenticação forte, preferencialmente autenticação multi-fator, e/ou a cifrar o dispositivo ou os dados sensíveis. O risco de acesso não autorizado aumenta caso não seja possível efetuar a limpeza (*wipe*) remota do dispositivo, disponível por exemplo através de soluções MDM. A formação e *awareness* contínuo pode igualmente ajudar a reduzir a postura dos utilizadores perante práticas de segurança física menos seguras.

Em termos de ii) dispositivos móveis, as ameaças mais inerentes são:

a) O uso de *malware* que permite que *hackers* infiltrem-se nos dispositivos e possam provocar danos, como o roubo de *passwords*, informações ou mesmo alterações prejudiciais. O acesso à internet a partir do dispositivo móvel está exposto ao risco de ameaças baseadas em web, assim como sempre que é efetuado o *download* de uma aplicação, existe igualmente o risco de instalar *software* com *malware* direcionado ao roubo de dados. Como medidas de mitigação podem ser consideradas: o uso de tecnologias *antimalware*, tais como software antivírus, *firewalls* e *passwords*; o uso de soluções NAC (*Network Access Control*); o recurso a redes separadas (e.g., rede própria para dispositivos externos); implementação de *container's* ("*sandboxs*") seguros nos dispositivos móveis onde corre o software da organização ou o recurso a aplicações de análise da integridade dos dispositivos.

b) A sincronização entre dispositivos que representa o risco de fuga dos dados, sendo uma ameaça de perda de propriedade intelectual, dados de negócio, dados pessoais, etc., na medida em que os colaboradores utilizam os seus dispositivos móveis no acesso aos dados da empresa, mas também para ligarem-se a outros sistemas, que podem estarem infetados. Uma situação comum é os computadores pessoais não terem as últimas atualizações de segurança instaladas o que possibilita que cibercriminosos explorem as vulnerabilidades e obtenham acesso aos dados guardados ou sincronizados nesses computadores. Atualmente verifica-se que cada vez mais os dispositivos estão preparados para partilharem informação através da *cloud*. Apesar de direcionada para o uso pessoal é certo que a maioria das pessoas também a usará para guardar dados corporativos que, por exemplo, necessitam de serem trabalhados fora do horário de expediente. A *cloud* é uma infraestrutura baseada em web, nalguns casos externa à organização (Dropbox, Goolge+ da Google, OneDrive da Microsoft) e que as organizações pouco ou nada controlam. No caso de existirem falhas na salvaguarda dos dados devido à implementação incorreta dos controlos internos, as organizações podem incorrer em incumprimento legal, ter prejuízos financeiros avultados, ou mesmo obter uma imagem negativa que poderá pôr em causa a continuidade da organização. As medidas de mitigação

podem passar novamente pela formação e *awareness* contínuo dos utilizadores e pela restrição ou proibição do uso de determinadas aplicações.

c) A proliferação de dispositivos móveis no mercado e o facto de rapidamente estes se tornarem obsoletos apresenta um risco na medida em que os departamentos de ICT podem não ter a capacidade de resposta em acompanhar as constantes alterações e de identificar os riscos associados dos novos dispositivos na ligação aos sistemas, pelo que importa restringir os dispositivos móveis, as versões e os sistemas operativos aceitáveis e cujo controlo é efetivo através por exemplo de soluções MDM.

d) A conformidade regulatória (lei e, ou regulamentação) mesmo quando a organização não é a proprietária do dispositivo. Um exemplo de uma não conformidade com as regras do uso de *software* e que pode levar a penalidades é o da utilização de software comprado para uso pessoal (licenciado para "*personal use*") que depois é usado em ambiente empresarial. Importa assegurar que os colaboradores estão informados desta situação, pelo que o processo de mitigação passa pela formação e *awareness*. Outra alternativa é considerar software ou serviços por assinatura (exemplo *SaaS*, Office 365, etc.).

Na componente iii) rede, a ameaça mais evidente relaciona-se com os mecanismos de conectividade usados, como por exemplo as tecnologias Bluetooth e Wi-Fi. Os dispositivos ligados entre si podem ganhar o acesso uns dos outros sem necessitarem de passarem pelo processo de autenticação. As ameaças são ainda maiores considerando que as tecnologias Bluetooth e WI-FI podem ser facilmente exploradas e suscetíveis a ataques de *eavesdropping* e de *Man-in-the-middle* (MITM). Como riscos verifica-se o comprometimento de dados assim como a possibilidade de interceção e modificação das comunicações. Como medidas de mitigação podem ser considerados o recurso a tecnologias de criptografia forte (como redes privadas virtuais, VPNs); a utilização de mecanismos de autenticação mútua que verifique a identidade nas duas extremidades antes da serem transmitidos os dados; a proibição do uso de redes Wi-Fi inseguras como por exemplo as que executam protocolos com vulnerabilidades conhecidas; e a desativação de interfaces de rede desnecessários, reduzindo assim a superfície de ataque.

Em termos de iv) aplicações, as ameaças ocorrem sobretudo com a instalação das aplicações web de terceiros, desenvolvidas por alguém que não conhecem. O software

instalado pode conter *malware* que pode permitir o roubo ou danificação dos dados do dispositivo e, até mesmo desabilitar o próprio dispositivo. Com a utilização dos dispositivos móveis no âmbito pessoal e profissional esta situação constitui uma ameaça para as organizações, na medida em que as aplicações não são adequadamente controladas e a maioria das pessoas não tem noção dos riscos de segurança que elas representam. Como medida de mitigação, as organizações podem proibir a instalação de aplicações de terceiros; estabelecer uma *whitelisting* das aplicações aprovadas; realizar avaliação de risco para cada aplicação de terceiros antes de permitir a utilização nos dispositivos móveis da organização; implementar *container's* ("*sandboxs*") seguros de forma a isolar os dados e aplicações da organização de todos os outros dados e aplicações no dispositivo móvel; disponibilizar o mínimo de acessos necessário de forma a restringir a propagação em caso de ameaça.

3.2 Análise Financeira BYOD

Não existe uma fórmula única da análise custo versus benefício e, principalmente que seja aplicável a todos as organizações. O BYOD é tido como um desenvolvimento positivo, com potenciais ganhos e redução de custos, no entanto têm surgido dúvidas em relação a esses benefícios. Se por um lado parecem existir ganhos na questão da produtividade, também é necessário considerar os custos de suporte.

As organizações devem adotar uma abordagem proactiva que possibilite a maximização dos benefícios e gerir em simultâneo os custos de implementação de uma infraestrutura de suporte à solução BYOD.

3.2.1 Benefícios BYOD

Um dos grandes benefícios da solução BYOD é o aumento da produtividade do colaborador e consequentemente o aumento das receitas (Lydon, 2014). O aumento de produtividade só ocorre se os colaboradores estiverem motivados. Sendo assim, um dos aspetos mais importantes é a predisposição dos colaboradores em aderirem a soluções BYOD. É necessário que as organizações percebam se os colaboradores estão dispostos ou se são contrários a uma solução deste tipo, pelo que é necessário avaliar o grau de maturidade da organização / colaboradores em relação à solução BYOD (Cisco IBSG, 2013).

Geralmente o BYOD é mais fácil de implementar nas organizações ou em áreas com perfil mais técnico, sendo mais difícil em áreas de cariz tradicional (como por exemplo, de recursos humanos, áreas financeiras ou administrativas, entre outras).

Numa primeira análise, a implementação de uma solução BYOD potencia benefícios em termos de aumento de produtividade:

- Aumento da satisfação do colaborador,
- Maior flexibilidade, e
- Aumento da iniciativa.

Assim temos o aumento de produtividade traduzido num melhor aproveitamento do tempo do colaborador. A Figura 3.1 ilustra os diferentes aspetos que podem contribuir para o aumento da produtividade decorrente da implementação duma solução BYOD, e que traduz-se na satisfação do colaborador, nomeadamente: i) maior predisposição do colaborador em utilizar dispositivos da sua preferência em vez dos dispositivos impostos pela organização (Nucleus Research, 2013; Cisco IBSG, 2013; Computer Weekly, 2012); ii) o que leva à diminuição do tempo despendido na aprendizagem, configuração e sincronização de um ou de vários dispositivos (Computer Weekly, 2012; Lydon, 2014); iii) a uma maior eficiência na utilização dos recursos, seja *software*, aplicações móveis, serviços de *cloud*, etc.; iv) e, a possibilidade dos colaboradores utilizarem os dispositivos pessoais do seu agrado para completarem as atividades de trabalho (Cisco IBSG, 2013).

Em termos de flexibilidade, verifica-se i) a possibilidade do colaborador ter acesso a informações corporativas mesmo estando fora do escritório, ii) podendo dar seguimento a questões do negócio, independentemente da sua localização geográfica (*anywhere / anyplace)* ou da hora do dia; iii) a autonomia em mover-se facilmente entre o trabalho e a vida pessoal e vice-versa a partir do mesmo dispositivo (Cisco IBSG, 2013); iv) na possibilidade de comunicar com outros colegas ou clientes que não estão próximos (sendo que os contactos estão igualmente no dispositivo pessoal em vez de estarem restritos ao computador que ficou na empresa).

Por iniciativa entende-se um potencial aumento do valor que o colaborador acrescenta para a organização (do tipo *bottom-up)* i) ao demostrar disponibilidade adicional; ii) na adoção de novas formas de trabalhar (Lydon, 2014) e iii) ao recorrer a ferramentas inovadoras (Cisco IBSG, 2013) em vez de limitar-se à escolha das ferramentas da organização, por vezes limitativas e ultrapassadas. Utilizar ferramentas novas, difundir o conhecimento dessas novas ferramentas pela organização, pode trazer

vantagens competitivas para as organizações sobretudo para as que situam-se em mercados mais ávidos por novidades e pelas novas tendências.

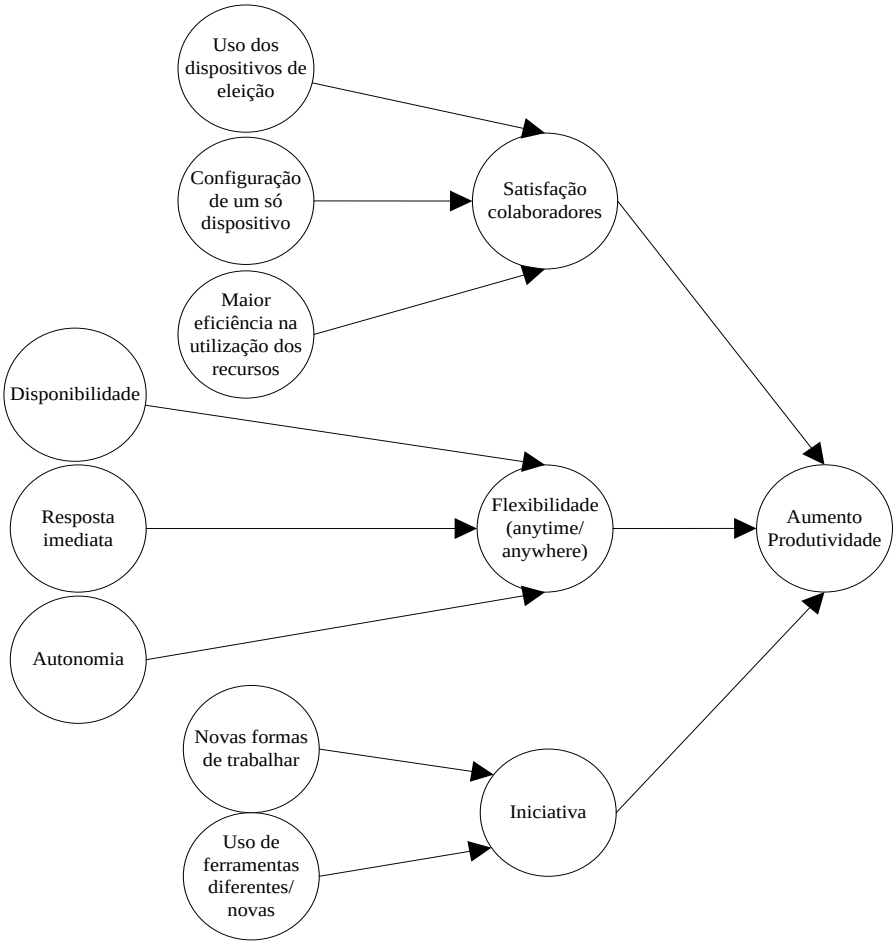

Figura 3.1 - Aspetos que contribuem para o aumento da produtividade

3.2.2 Custos BYOD

A implementação de uma solução BYOD pode afetar diferentes tipos de despesas, podendo existir situações de aumento de custos e, em outras, uma diminuição dos mesmos. O aumento ou a diminuição do custo de implementação da solução BYOD vai depender sobretudo de como a organização funciona, se é nova no conceito BYOD, se já considera o BYOD para alguns dispositivos ou se já possui inclusive infraestruturas de suporte ao BYOD (Computer Weekly, 2012).

As áreas chave onde a despesa tende a aumentar são na grande maioria relacionadas com a infraestrutura de suporte e, com o desenvolvimento e segurança das aplicações corporativas. Em relação à diminuição da despesa, verificam-se sobretudo nas componentes relacionadas com os custos de compra e substituição dos dispositivos, e nas despesas com serviços de telecomunicações. Como podemos observar na Figura

3.2, em termos de infraestrutura de suporte a soluções BYOD, as empresas devem considerar custos com:

i) a utilização de soluções de gestão de dispositivos móveis (*Mobile Device Management* – MDM, *Telecom Expense Management* - TEM ou *Enterprise Mobility Management* - EMM) (Cisco IBSG, 2013; Nucleus Research, 2013; Lydon, 2014; Arregui, 2015), que permite não só monitorizar como "limpar" os dados corporativos dos dispositivos móveis em caso de necessidade, assim como implementar remotamente políticas de segurança e gerir custos;

ii) a adesão ou a criação de infraestruturas de serviços *cloud computing* como alternativa de armazenamento e suporte aos dados corporativos (Cisco IBSG, 2013);

iii) alterações à rede, como por exemplo a criação de VPNs (*Virtual Private Network*) de forma a permitir o acesso seguro à infraestrutura corporativa e a implementação de redes Wi-Fi seguras (Cisco IBSG, 2013; Lydon, 2014), e

iv) o alargamento da atual infraestrutura devido ao aumento de utilizadores BYOD (Computer Weekly, 2012) (utilização e ligação à rede a partir de vários dispositivos em simultâneo).

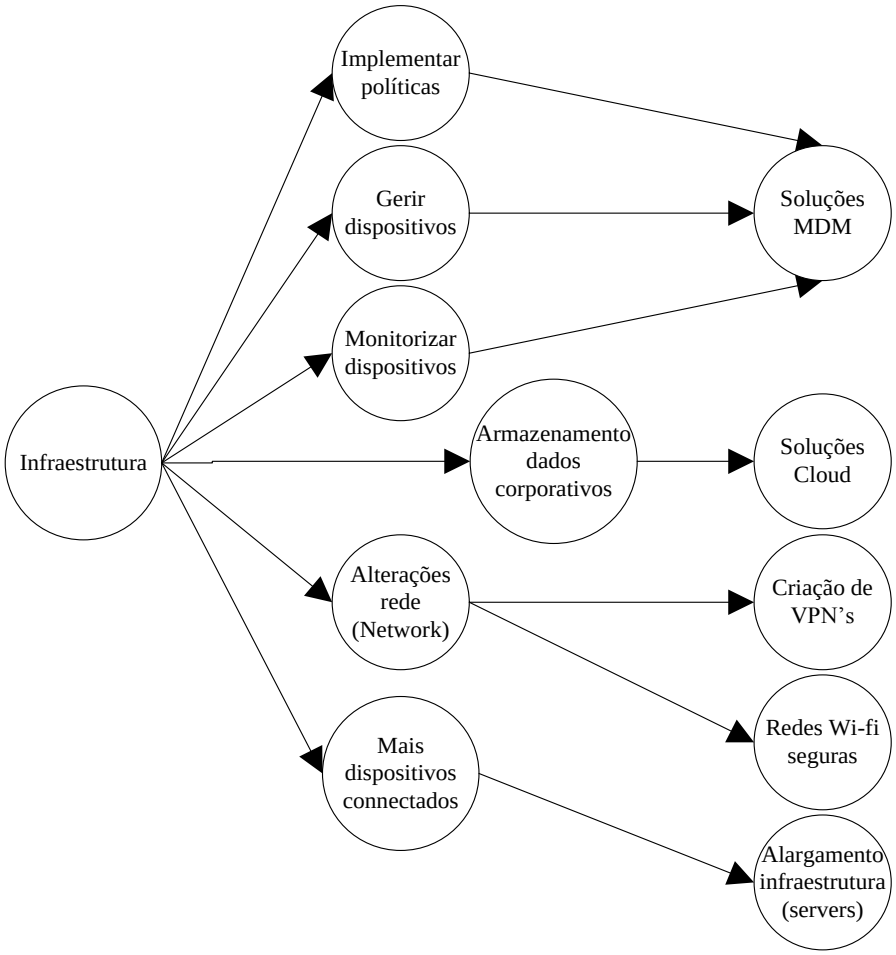

Figura 3.2 - Custos com a infraestrutura de suporte

Na Figura 3.3 são ilustrados custos com aplicações corporativas, nomeadamente:

i) o desenvolvimento e adaptação das aplicações corporativas face aos dispositivos móveis autorizados (Computer Weekly, 2012; Nucleus Research, 2013), sendo que as aplicações necessitam de ser compatíveis consoante os dispositivos usados (pelo que importa limitar o tipo/modelo de dispositivos autorizados); e

ii) o licenciamento do software (Cisco IBSG, 2013) usado nos dispositivos móveis (sendo uma alternativa a disponibilização do software corporativo numa plataforma *Software as a Service* - *SaaS*, como por exemplo Office 365).

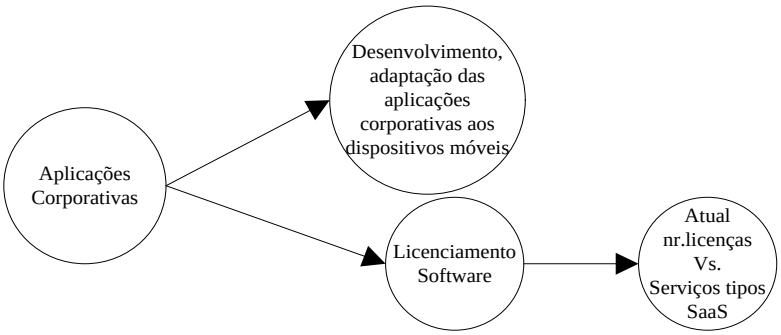

Figura 3.3 - Custos com aplicações corporativas

Ainda decorrente da implementação duma solução BYOD, e conforme observado na Figura 3.4 é necessário avaliar custos de suporte e formação:

i) com o desenvolvimento de uma política BYOD (Cisco IBSG, 2013; Nunoo, 2013; Lydon, 2014; Agudelo et al., 2015);

ii) com o desenvolvimento de programas *awareness* específicos e direcionados (Cisco IBSG, 2013; Lydon, 2014; Agudelo et al., 2015); e

iii) com o suporte *help-desk*, (Cisco IBSG, 2013; Nucleus Research, 2013), podendo no entanto considerar-se um ganho, caso exista alteração da tradicional abordagem de *help-desk* para uma abordagem mais autónoma com recurso a mecanismos do tipo "suporte a comunidades" através da divulgação de *wikis* e, ou de fóruns de discussão internos (Computer Weekly, 2012). Estas mudanças dependem sobretudo do nível de aceitação e do tipo de colaboradores (mais ou menos adeptos às novas tecnologias).

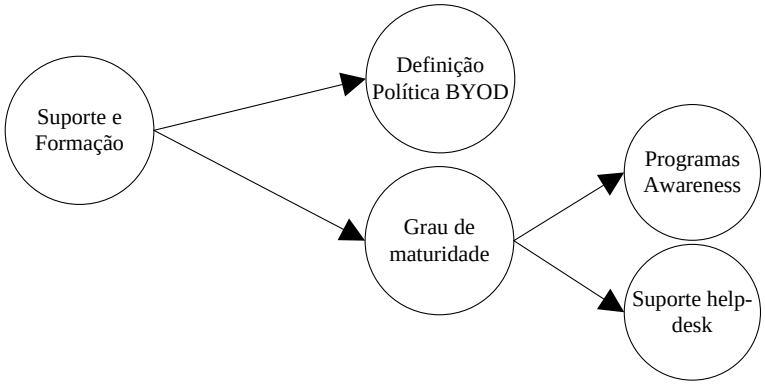

Figura 3.4 - Custos com suporte e formação

Em relação aos dispositivos e telecomunicações, sendo o BYOD uma solução em que o dispositivo é maioritariamente do colaborador, as organizações podem diminuir custos relacionados. Na Figura 3.5 são ilustrados os aspetos que podem contribuir para a diminuição dos custos, considerando custos atuais. Há que considerar os custos:

i) com a compra dos dispositivos corporativos. (Nas organizações mais tradicionais, isto é, em que os dispositivos pertencem à organização e, em que o custo é totalmente suportado pela mesma, pode ser uma vantagem, sendo que este custo pode deixar de existir (Lydon, 2014) ou pode ser dividido através de programas que consideram a definição de uma comparticipação na compra dos dispositivos pessoais. No entanto, pode significar uma desvantagem, uma vez que geralmente existem descontos para as organizações, baseado por exemplo no número de unidades adquiridas (Cisco IBSG, 2013; Computer Weekly, 2012; Nucleus Research, 2013);

ii) com a substituição dos dispositivos, sendo que tende a existir, por parte do colaborador, uma maior preocupação com a manutenção e proteção dos equipamentos pessoais do que com os equipamentos corporativos; e

iii) com as telecomunicações, uma vez que pode ser possível migrar o plano de dados corporativos para um plano de dados que os colaboradores já possuem (no entanto é necessário considerar, uma vez mais se esta situação é contrária, tendo em conta os descontos obtidos pelas organizações quando celebram planos corporativos com os operadores), sendo que também pode ser visto como um custo caso seja necessário estabelecer planos de dados (que anteriormente não existiam) (Computer Weekly, 2012).

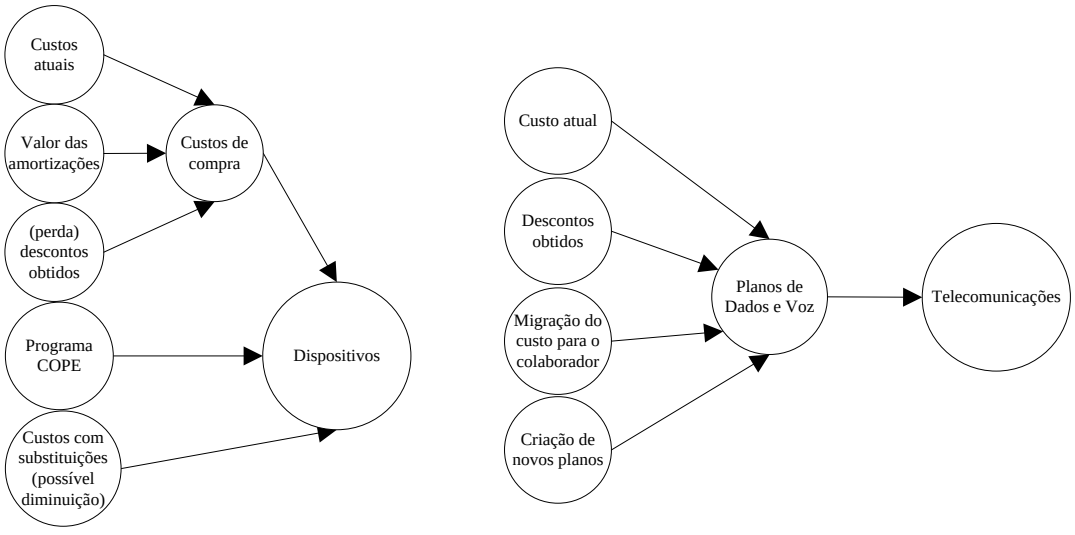

Figura 3.5 - Custos com dispositivos e com planos de telecomunicações

Numa fase inicial existem grandes expectativas em relação aos benefícios da solução BYOD. Com o decorrer da implementação e com a maturidade do processo, obtém-se eficiência operacional em que os benefícios podem superar os custos de

implementação da solução BYOD, caso tenha sido efetuado uma análise custo-benefício realista.

3.3 Resumo

O BYOD tem vindo a ser implementado nas organizações. A falta de uma abordagem estratégica cria riscos de segurança, exposição financeira e problemas para a gestão ICT. Em vez de resistir há que tirar partido do seu potencial. Desta forma há que definir qual a melhor abordagem estratégica, políticas flexíveis e implementar as ferramentas de gestão e de segurança mais adequadas. Neste capítulo foi efetuada a revisão da literatura o que permitiu efetuar o enquadramento da implementação de uma solução BYOD e detalhar as situações e cenários mais comuns presentes em soluções BYOD. A questão legal assume relevância tendo em conta tratar-se de um modelo que ainda não está previsto na legislação portuguesa aplicando-se por isso *mutatis mutandis* (ou seja, a analogia ao que existe considerando as devidas proporções e alterações necessárias), (Costa, 2015). Desta forma foi efetuado um levantamento (embora superficial) da legislação portuguesa de forma a responder à pergunta Q3. Requisitos legais que podem influenciar a solução BYOD?.

Recolhendo informação sobre as ameaças mais emergentes na solução BYOD, foram encontrados cenários que permitiram desenvolver e documentar a questão Q4. Que riscos estão presentes na implementação de uma solução BYOD?.

Por último e após a recolha da informação referente aos requisitos legais, e dos diferentes cenários de ameaças e possíveis soluções de mitigação, foram encontrados alguns fatores que podem contribuir para a análise custo versus benefício, respondendo dessa forma à pergunta Q5. Quais os benefícios e custos presentes na solução BYOD?

Com base na informação acima referida é possível responder à questão Q6. O que considerar na elaboração de uma Política de Segurança BYOD?, sendo no Capítulo 4 apresentada uma proposta de documentação sobre os elementos que devem ser considerados na elaboração da Política de Segurança BYOD. Propõe-se também um modelos de suporte à tomada de decisão na adoção de uma solução BYOD. De referir que a Política de Segurança BYOD deve ser elaborada tendo em conta as soluções de mitigação adaptadas pela organização.

Capítulo 4

Modelo de suporte à decisão para apreciação de solução BYOD

Neste capítulo apresenta-se o modelo de suporte à decisão para avaliação da solução BYOD sendo composto por vários modelos, nomeadamente um Modelo de análise dos Requisitos Legais Obrigatórios (MRLO); um Modelo de Avaliação dos Riscos (MAR) através da análise dos ativos e das potenciais ameaças; um Modelo que permite estabelecer o Posicionamento ICT (MPICT); um Modelo de ações relacionadas com custo-benefício (CBA) (MCBA); e um Modelo para o estabelecimento de uma Política de Segurança BYOD (MCPSB).

Na Figura 4.1 podemos observar o relacionamento entre os vários modelos, sendo que os três primeiros modelos (MRLO, MAR e MPICT) podem ser desenvolvidos paralelamente e referem-se sobretudo à recolha de informação. O modelo MCBA e MCPSB são modelos sequenciais, sendo que o modelo MCBA é estabelecido com base nos *inputs* dos anteriores três modelos, servindo posteriormente também de *output* para o modelo MCPSB, caso o parecer da solução BYOD seja favorável.

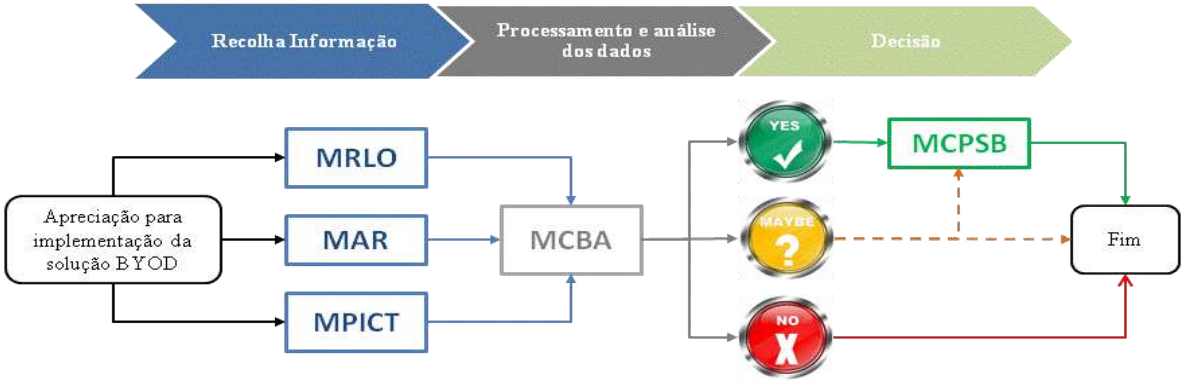

Figura 4.1 - Relacionamento entre os modelos

Recorrendo ao modelo proposto é possível estruturar a informação de forma a organizar e documentar os diferentes requisitos necessários (legais, operacionais e financeiros) para a avaliação da implementação de uma solução BYOD. Na Figura 4.2 podemos observar o modelo de domínio tendo utilizado a linguagem *UML(Unified Modeling Language).*

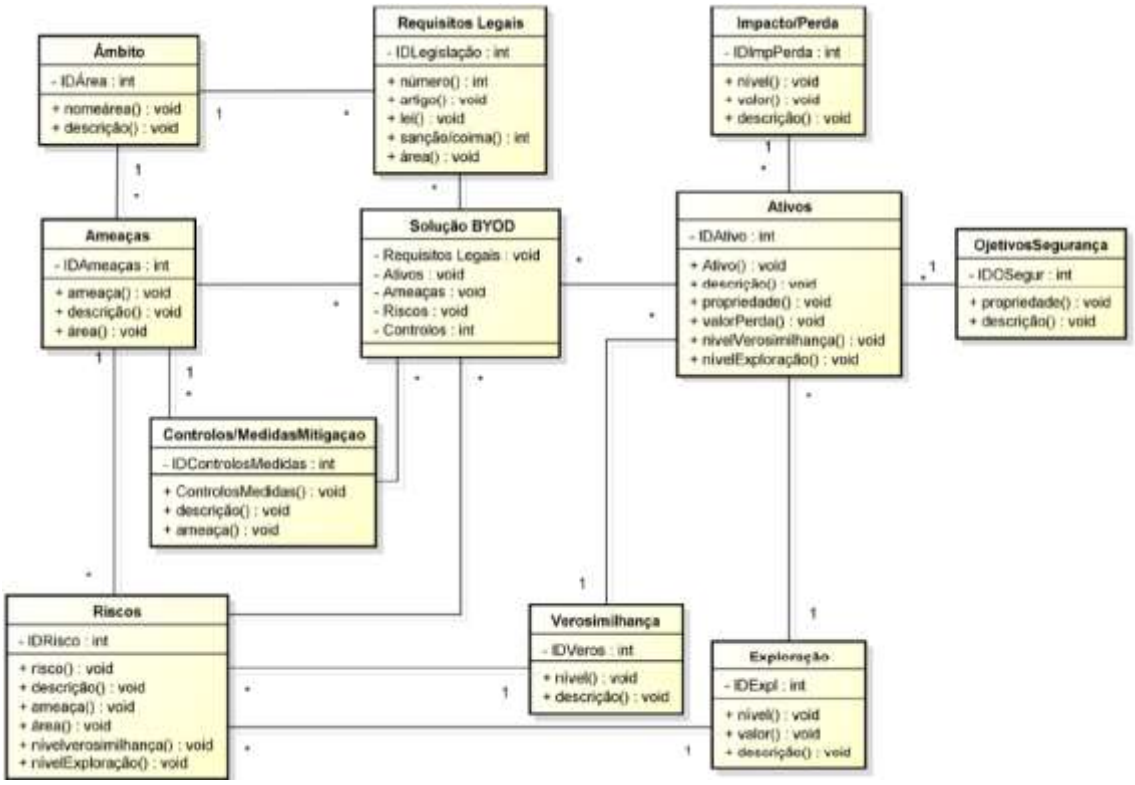

Figura 4.2 - Modelo de domínio

Os modelos foram desenvolvidos em Excel e encontram-se disponíveis em: https://meocloud.pt/link/fe2f3896-01d9-4c6b-b316-824163aeb197/FCUL%20-%20Disserta%C3%A7%C3%A3o%20MSI%2045478/ ou https://o31gqa.s.cld.pt.

4.1 Modelo de análise dos Requisitos Legais Obrigatórios (MRLO)

O contexto para a implementação de uma solução BYOD pode ser determinado de diversas maneiras. Para o modelo apresentado foi estabelecido considerando o levantamento da legislação e da identificação do envolvimento das áreas que devem pronunciarem-se sobre a implementação da solução BYOD. No Anexo B, baseado no levantamento de informação do Capítulo 3, estão identificadas sete áreas onde a legislação portuguesa pode ter influência na implementação de uma solução BYOD.

Com base nessas áreas foi estabelecido: i) os requisitos legais obrigatórios; ii) as possíveis soluções; e iii) o envolvimento das áreas.

Em termos de envolvimento a área Jurídica tem como missão efetuar o levantamento dos requisitos legais; a área de ICT tem como objetivo estabelecer as ameaças, os riscos e as possíveis medidas de mitigação; e a área de Recursos Humanos deverá estabelecer pareceres sobretudo relacionados com produtividade, pagamentos e custos laborais; no processo de consentimento dos colaboradores e, no estabelecimento dos direitos, deveres e consequências por utilizações incorreta.

Na Tabela 4.1, e com base nas áreas de atuação onde a legislação portuguesa pode ter influência, foi desenvolvido o modelo para registo e análise dos requisitos legais obrigatórios. O objetivo deste modelo é registar a legislação aplicável para cada grupo estabelecendo dessa forma a relação entre a legislação e a solução BYOD.

Instruções de Preenchimento:
Passo 1: *Preencher cabeçalho (data e a identificação, por exemplo, email corporativo).*
Passo 2: *Preencher com um "x" caso a situação seja "Aplicável" ou "Não Aplicável".*
Passo 3: *Preencher na coluna "informação" os dados referentes às questões.*
Passo 4: *Classificar de 1 a 7 o grupo prioritário.*

Data:

Efetuado por:

Grupo	Questões	A	NA	Informação	Priorização
1. Proteção dos dados sensíveis corporativos	a) Legislação aplicável: (número x, artigo x, Lei x)				
	b) Sanções/Coimas (especificar):				
	c) Comentários:				
2. Possíveis quebras de segurança	a) Legislação aplicável: (número x, artigo x, Lei x)				
	b) Sanções/Coimas (especificar):				
	c) Comentários:				
3. Regulação e legislação aplicável	a) Sector de atividade:				
	b) Legislação aplicável: (número x, artigo x, Lei x)				
	c) Sanções/Coimas (especificar):				
	d) Comentários:				
4. Requisitos legais aplicáveis aos territórios	a) Localização/Território:				
	b) Legislação aplicável: (número x, artigo x, Lei x)				
	c) Sanções/Coimas (especificar):				
	d) Comentários:				
5. Proteção dos dados pessoais	a) Legislação aplicável: (número x, artigo x, Lei x)				
	b) Sanções/Coimas (especificar):				
	c) Comentários:				
6. Licenciamento de software e penalidades	a) Legislação aplicável: (número x, artigo x, Lei x)				
	b) Sanções/Coimas (especificar):				
	c) Comentários:				
7.Riscos laborais	a) Legislação aplicável: (número x, artigo x, Lei x)				
	b) Sanções/Coimas (especificar):				
	c) Comentários:				

A = Aplicável; NA = Não aplicável

Tabela 4.1 - Modelo para registo e análise dos requisitos legais obrigatórios (MRLO)

Este modelo vai permitir analisar a questões legais relacionadas com a implementação da solução BYOD e priorizar por exemplo em termos tecnológicos as áreas de maior relevância face aos valores monetários das sanções ou coimas.

4.2 Modelo para Avaliação dos Riscos (MAR)

Considerando os pilares da segurança da informação (confidencialidade, integridade e disponibilidade, conforme descritos no Capítulo 1) importa estabelecer o significado da perda desses objetivos (NIST, 2008). Assim temos:

Perda da Confidencialidade - divulgação não autorizada de informações;

Perda da Integridade - modificação ou destruição não autorizada de informações;

Perda da Disponibilidade - interrupção do acesso, do uso de informações ou do sistema de informação.

De seguida e baseado igualmente no NIST (2008), é estabelecido o nível de potenciais impactos. Na Tabela 4.2 é proposto três níveis de potenciais impactos para a perda dos objetivos de segurança. Para cada nível de impacto foram atribuídos valores quantitativos (entre um e três, sendo um o valor mais baixo, e três o valor mais alto), o que vai permitir estabelecer o valor ao ativo.

Níveis	Valor	Descrição
Baixo	1	**Perda da Confidencialidade, Integridade e Disponibilidade:** Efeito adverso limitado sobre as operações organizacionais, ativos ou indivíduos. Pode provocar: i) Degradação da capacidade da missão e redução da eficácia de funções durante o período de tempo, no entanto a organização continua a conseguir desempenhar as suas funções primárias; ii) danos menores aos ativos; iii) prejuízo financeiro menor; iv) danos menores para os indivíduos.
Moderado	2	**Perda da Confidencialidade, Integridade e Disponibilidade:** Efeito adverso grave sobre as operações organizacionais, ativos ou indivíduos. Pode provocar: i) Degradação significativa da capacidade da missão e redução significativa da eficácia de funções durante o período de tempo, no entanto a organização é capaz de desempenhar suas funções primárias; ii) danos significativos aos ativos; iii) perda financeira significativa, iv) danos significativos para os indivíduos (sem envolver perda de vida ou lesões graves que ameaçam a vida).
Alto	3	**Perda da Confidencialidade, Integridade e Disponibilidade:** Efeito adverso grave ou catastrófico sobre as operações, ativos organizacionais ou indivíduos. Pode provocar: i) degradação ou perda da capacidade da missão durante o período de tempo, e em que a organização não é capaz de desempenhar uma ou mais das suas funções primárias; ii) grandes danos aos ativos; iii) grandes perdas financeiras; iv) danos grave ou catastrófico para os indivíduos (envolvimento de perda de vidas ou ferimentos graves com risco de vida).

Tabela 4.2 - Potencial impacto

Desta forma estão criadas condições para estabelecer o valor do ativo (ISO/IEC, 2011). Na Tabela 4.3 é apresentado o modelo de classificação do ativo face à perda dos objetivos de segurança.

Para cada ativo foi estabelecido o valor relativo que a provável perda dos objetivos de segurança terá sobre o mesmo.

Instruções de Preenchimento:
Passo 1: *Preencher a coluna "Nome do ativo" com o nome do ativo devendo o mesmo ser o mais explicito possível(distinguir se é um portal, base de dados, aplicação, etc.).*
Passo 2: *Preencher as colunas "Confidencialidade", "integridade" e "Disponibilidade" com base na classificação fornecida: baixo, moderado, alto.*
NOTAS: *O valor do ativo é atribuído automaticamente baseado no nível de impacto aplicado aos requisitos de segurança. Pode ir de 3 a 9.*

#	Nome do Ativo	Confidencialidade	Integridade	Disponibilidade	Valor do Ativo
1	site interno corporativo	baixo	baixo	baixo	3
2	site externo	moderado	moderado	moderado	6
3	email corporativo	alto	baixo	moderado	6
4	bd aplicação vendas	alto	alto	alto	9

Tabela 4.3 - Modelo valor do ativo

Uma vez que para cada valor relativo foi associado um valor quantitativo, podemos concluir que um ativo cujos requisitos de segurança sejam baixos, isto é, Confidencialidade = baixo (= um), Integridade = baixo (= um), Disponibilidade= baixo (= um), será um ativo com um valor baixo (igual a três). No exemplo seguinte, o ativo foi classificado com o valor seis, sendo que a perda dos objetivos de segurança situam-se todos no nível moderado, isto é, Confidencialidade = moderado (= dois), Integridade = moderado (= dois), Disponibilidade = moderado (= dois).

No modelo proposto e, tendo sido estabelecido os valores entre um (baixo) e três (alto) na relação com os objetivos de segurança, o valor máximo que um ativo pode atingir é de nove (exemplo do ativo identificado na linha quatro da Tabela 4.3).

Encontrado o valor do ativo passamos para a análise de risco. Assim numa primeira fase é necessário identificar as prováveis ameaças e estabelecer uma classificação quanto à sua verosimilhança de ocorrência e facilidade de exploração.

Na Tabela 4.4 e na Tabela 4.5 são propostos diferentes níveis de classificação para a verosimilhança de ocorrência de ameaças e para a facilidade de exploração das mesmas, adaptado do NIST (2012).

Níveis	Descrição
Muito Alto	Probabilidade muito alta de uma determinada ameaça ocorrer face a uma vulnerabilidade ou conjunto de vulnerabilidades.
Alto	Probabilidade alta de uma determinada ameaça ocorrer face a uma vulnerabilidade ou conjunto de vulnerabilidades.
Baixo	Probabilidade baixa de uma determinada ameaça ocorrer face a uma vulnerabilidade ou conjunto de vulnerabilidades.
Muito Baixo	Probabilidade mínima de uma determinada ameaça ocorrer face a uma vulnerabilidade ou conjunto de vulnerabilidades.

Tabela 4.4 - Verosimilhança de ocorrência

Níveis	Valor	Descrição
Crítico	C	A vulnerabilidade está exposta e pode ser explorada, sendo que a sua exploração pode ter um impacto crítico. Não estão implementados ou planeados controlos de segurança relevantes ou outras medidas de mitigação. Não foram identificadas medidas de segurança que permitam mitigar a vulnerabilidade.
Severo	S	A vulnerabilidade é preocupante face à sua exposição, facilidade de exploração e/ou na gravidade dos impactos que daí podem advir. Os controlos de segurança ou outras medidas de mitigação estão planeados, mas não estão implementados. Existem medidas de segurança eficazes que permitem mitigar a vulnerabilidade.
Moderado	M	A vulnerabilidade é de preocupação moderada face à sua exposição, facilidade de exploração e/ou na gravidade dos impactos que daí podem advir. Os controlos de segurança ou outras medidas de mitigação estão parcialmente implementados e são eficazes.
Baixo	B	A vulnerabilidade é de preocupação baixa face à sua exposição, facilidade de exploração e/ou na gravidade dos impactos que daí podem advir. Os controlos de segurança ou outras medidas de mitigação estão completamente implementados e são eficazes.

Tabela 4.5 - Facilidade de exploração

Sendo o valor da verosimilhança associado à estimativa de probabilidade, o termo probabilidade será usado para representar essa estimativa.

Conforme descrito no Capítulo 3, estabeleceu-se um cenário de ameaças versus risco agrupado nas quatro áreas principais: 1. Segurança física; 2. Dispositivos móveis; 3. Rede; e 4. Aplicações.

Na Tabela 4.6 é proposto o modelo de ameaças e risco (MAR), onde foi relacionado os diferentes cenários de ameaças com as classificações da Tabela 4.4 e da Tabela 4.5.

Instruções de Preenchimento:
Passo 1: *Preencher na coluna "Probabilidade de Ocorrência" o nível de impacto da ameaça, considerando os valores: Muito Baixo; Baixo; Alto; Muito Alto*
Passo 2: *Preencher na coluna "Facilidade de Exploração" o nível de impacto da ameaça, considerando os valores: Baixo, Moderado, Severo, Crítico.*

Áreas	Cenários de ameaças ICT		Ameaça versus	
	Ameaças	**Risco**	**Probabilidade de Ocorrência**	**Facilidade de Exploração**
1. Segurança Física	• Roubo ou perda de dispositivos móveis	• Comprometimento dos dados • Acesso não autorizado	Muito Alto	Severo
2. Dispositivos móveis	• *Malware*	• Acesso não autorizado • Integridade dos dados • Roubo de dados	Alto	Severo
	• Sincronização entre dispositivos	• Fuga dos Dados • Roubo de dados negócio e pessoais • Perda de propriedade intelectual • Imagem negativa • Prejuízos financeiros	Alto	Moderado
	• Proliferação de dispositivos móveis	• Equipamentos obsoletos • Incapacidade de resposta ICT para as alterações	Baixo	Baixo
	• Utilização de software não licenciado	• Penalidades e coimas	Alto	Severo
3. Rede	• Mecanismos de conectividade inseguros: *Bluetooth* e *Wi-Fi*	• Interceção e modificação das comunicações • Acesso não autorizado	Muito Alto	Crítico
	• Ataques*: Eavesdropping* e *Man-in-the-middle (MITM)*	• Comprometimento de dados	Alto	Severo
4. Aplicações	• Acesso externo a recursos internos	• Comprometimento dos recursos internos (Ex: servidores)	Alto	Severo

Tabela 4.6 - Modelo de ameaças versus probabilidade de ocorrência e facilidade de exploração (MAR)

Para cada cenário de ameaça foi atribuído a respetiva classificação do nível de probabilidade de ocorrência e do nível de facilidade de exploração.

De forma a concluir o modelo de análise de risco foi elaborado na Tabela 4.7 uma matriz de risco, baseado na ISO 27005:2011 (ISO/IEC, 2011). Assim, ao relacionarmos o modelo valor do ativo (Tabela 4.3) com o modelo de ameaças e risco (Tabela 4.6) e recorrendo à matriz proposta, obtemos o posicionamento do ativo face ao risco de ameaça.

Ameaça vs Probabilidade de Ocorrência		Muito Baixo				Baixo				Alto				Muito Alto			
Facilidade de Exploração		B	M	S	C	B	M	S	C	B	M	S	C	B	M	S	C
Valor do Ativo	0	0	1	2	3	1	2	3	4	2	3	4	5	3	4	5	6
	1	1	2	3	4	2	3	4	5	3	4	5	6	4	5	6	7
	2	2	3	4	5	3	4	5	6	4	5	6	7	5	6	7	8
	3	3	4	5	6	4	5	6	7	5	6	7	8	6	7	8	9
	4	4	5	6	7	5	6	7	8	6	7	8	9	7	8	9	10
	5	5	6	7	8	6	7	8	9	7	8	9	10	8	9	10	11
	6	6	7	8	9	7	8	9	10	8	9	10	11	9	10	11	12

B=Baixo; M=Moderado; S=Severo; C=Critico

Tabela 4.7 - Matriz de Risco

Assim, segundo o exemplo assinalado, o ativo "4. bd aplicação de vendas", atinge o valor mais elevado da matriz de risco (doze), uma vez que a ameaça é "Muito Alto" quanto à probabilidade de ocorrência e "Crítico" quanto à facilidade de exploração, o que coloca este ativo com um risco elevado, perante o cenário de ameaça em concreto.

Com base nestes modelos é possível fazer uma análise dos ativos, estabelecer a criticidade dos mesmos, definir ou excluir os ativos da solução BYOD, limitar a solução BYOD a determinados dispositivos móveis ou a determinadas áreas e identificar o nível de risco dos ativos expostos à implementação da solução BYOD.

4.3 Modelo de Posicionamento ICT (MPICT)

Com base no cenário de ameaças versus risco foi efetuado o levantamento dos possíveis controlos de segurança e/ou medidas de mitigação conforme descrito no Capítulo 3 e disponibilizado no Anexo C. Foram consideradas três áreas principais de negócio: 1. "Sistemas de informação", relacionado com pessoas, desenvolvimento de processos e procedimentos; 2. "N*etwork"*, relacionados com as questões de rede; e 3. "S*oftware"*, relacionados com aplicações e engenharia de software. De referir que considerou-se o *hardware* como sendo um componente interno da área "*owner* do controlo", sendo da sua responsabilidade definir e incluir a necessidade de *hardware* adicional.

Na Tabela 4.8 é proposta a estrutura do modelo de análise do posicionamento ICT.

Modelo de posicionamento das ameaças versus controlos de segurança e/ou medidas de mitigação ICT				
1.Análise		2.Situação atual	3.Impacto no negócio	4.Esforço de implementação
A	NA	<Existe | Implementar>	Valor	Valor

Tabela 4.8 - Estrutura do modelo de posicionamento ICT

Assim sendo, o modelo de análise do posicionamento ICT (abreviado para Modelo de posicionamento ICT, ou MPICT) é composto por quatro fases onde em cada uma delas se analisa uma área principal:

1. A área análise, onde para os itens identificados nos controlos de segurança e/ou medidas de mitigação, deve ser referido se são "A (aplicáveis)" ou "NA (não aplicáveis)", estabelecendo-se desta forma as opções quanto aos cenários de ameaças versus controlos de segurança e/ou medidas de mitigação;

2. A área situação atual, onde para os itens identificados no passo anterior como "A (aplicáveis)", os controlos de segurança e/ou medidas de mitigação estão completamente implementados, i.e. se existem: "Existe" ou se requerem implementação: "Implementar". Um controlo de segurança ou medida de mitigação parcialmente implementado mas que não responde na totalidade ao controlo de segurança deve ser considerado como por "Implementar". Por outro lado, se o controlo é parcial mas eficaz, deve ser considerado como "Existe". Após o preenchimento destas duas áreas, todos os itens "NA (não aplicáveis)" e "Existe" deixam de ter relevância para as fases seguintes.

3. A área impacto no negócio, onde para cada item identificado no passo anterior como a "Implementar", deve ser atribuído um valor de impacto do controlo de segurança e/ou a medida de mitigação no negócio. O preenchimento desta fase é suportado no modelo de análise de impacto geralmente estabelecido nas organizações aquando da elaboração do processo *Business Impact Analysis* (BIA), desencadeando no âmbito do plano de continuidade de negócio

4. A área esforço de implementação, onde para cada item identificado na fase dois como "Implementar", deve ser atribuído o valor de esforço de implementação, geralmente relacionados com as duas categorias básicas de despesas comerciais: *capital expenditures* (CAPEX) e *operating expenses* (OPEX).

Não sendo âmbito da dissertação o processo BIA e o estabelecimento de despesas comerciais (CAPEX/OPEX) disponibiliza-se no Anexo D uma tabela com valores fictícios anuais de impacto no negócio e de esforço de implementação, que serviu de suporte ao preenchimento dos valores referente às fases três e quatro do modelo proposto. Estes valores devem ser adaptados para cada organização.

Na Tabela 4.9 é proposto o modelo de posicionamento ICT (MPICT) preenchido e relacionado com o modelo de ameaças MAR (Tabela 4.6) versus os controlos de segurança e/ou medidas de mitigação (anteriormente disponibilizado no Anexo C).

Instruções de Preenchimento:

Passo 1: *Marcar com "X" as colunas "A (Aplicável)" ou "NA (Não aplicável)" para cada item identificado na coluna " Possíveis medidas de Mitigação".*

Passo 2: *Para cada item com "X" em "A (Aplicável)" preencher na "Situação Atual" se a medida de mitigação "E (Existe)" ou se requer Implementação "I (Implementar)".*

Passo 3: *Para cada item "I (implementar)", preencher na coluna "Impacto no Negócio" o valor (de 1 a 5) correspondente na tabela auxiliar de "Valores de Impacto no Negócio" considerando o valor anual expectável.*

Passo 4: *Novamente para cada item identificado na "Situação Atual" de "implementar", preencher na coluna "Esforço de Implementação" o valor (de 1 a 5) correspondente na tabela auxiliar de "Valores de Esforço de Implementação" considerando o valor CAPEX / OPEX anual expectável.*

NOTAS:

- *As colunas sombreadas na área destinada ao Modelo de posicionamento das ameaças versus medidas de mitigação IT são relativas a fórmulas pelo que não devem ser alteradas, exceto se for identificado algum erro no código.*
- *Sempre que se verifique situações de incompatibilidade entre colunas, os erros são assinaladas numa cor diferente (exemplo: a vermelho).*

Áreas	Cenários de ameaças IT				Controlos de Segurança e/ou Medidas de Mitigação		Modelo de posicionamento das ameaças vs. controlos/medidas				
			Ameaça versus				1.Análise		2.Situação Atual		
	Ameaças	Risco	Probabilidade de Ocorrência	Facilidade de Exploração	Descrição	Área de atuação	A	NA	Existe | Implementar	3.Impacto no Negócio	4.Esforço de Implementação
1. Segurança Física	• Roubo ou perda de dispositivos móveis	• Comprometimento dos dados • Acesso não autorizado	Muito Alto	Severo	• Autenticação forte	software		x			
					• Autenticação multi-fator	software	x		implementar	3	3
					• Cifrar o dispositivo ou os dados sensíveis	software	x		existe		
					• Limpeza *(wipe)* remoto (Solução MDM)	software	x		implementar	3	4
					• Formação e *Awareness* (roubo e perda)	si	x		implementar	1	1
2. Dispositivos móveis	• *Malware*	• Acesso não autorizado • Integridade dos dados • Roubo de dados	Alto	Severo	• Tecnologias antimalware: software antivírus, *firewalls* e passwords	software	x		implementar	2	2
					• Soluções NAC (*Network Access Control*) ou EVA (*Endpoint Visibility, Access, and Security*);	network		x			
					• Redes separadas (rede própria para dispositivos externos, em vez de acederem diretamente à rede interna)	network	x		implementar	3	3
					• Aplicações de análise da integridade dos dispositivos	software		x			

	• Sincronização entre dispositivos	• Fuga dos Dados	Alto	Moderado	• Formação e *Awareness* (sincronização entre dispositivos)	si	x		implementar	1	1
		• Roubo de dados negócio e pessoais			• Restrição e ou proibição do uso de determinadas aplicações	si	x		existe		
		• Perda de propriedade intelectual • Imagem negativa • Prejuízos financeiros			• Serviços de *Cloud Computing*	network	x		existe		
	• Proliferação de dispositivos móveis	• Equipamentos obsoletos • Incapacidade de resposta ICT para as alterações	Baixo	Baixo	• Restrição dos dispositivos móveis, versões e sistemas operativos com controlo efetivo	si	x		implementar	2	1
	• Utilização de software não licenciado	• Penalidades e coimas.	Alto	Severo	• Disponibilização de software e, ou serviços por assinatura (exemplo: SAAS, Office 365, etc.)	software	x		implementar	2	3
					• Formação e *Awareness* (licenciamento)	si	x		implementar	1	1
3. Rede	• Mecanismos de conectividade inseguros: *Bluetooth* e *Wi-Fi*	• Interceção e modificação das comunicações • Acesso não autorizado • Comprometimento de dados	Muito Alto	Critico	• Criptografia forte (como redes privadas virtuais, VPNs)	network	x		implementar	3	3
					• Mecanismos de autenticação mútua (verificação da identidade em ambos os *endpoints*) (Solução NAC ou EVA)	network	x		implementar	3	4
	• Ataques: Eavesdropping e Man-in-the-middle (MITM)		Alto	Severo	• Proibição do acesso a redes Wi-Fi inseguras, i.e., que executam protocolos com vulnerabilidades conhecidas	si	x		implementar	3	1
					• Desativação de interfaces de rede desnecessários	network	x		implementar	3	1
4. Aplicações	• Acesso externo a recursos internos	• Comprometimento dos recursos internos (Ex: servidores)	Alto	Severo	• Disponibilização do mínimo (acessos) necessário	si	x		existe		
					• Proibição da instalação de aplicações de terceiros	si	x		implementar	2	1
					• Criação de *whitelisting* das aplicações aprovadas	si	x		implementar	2	1
					• Implementação de *sandbox's/containers seguros* que isola os dados e as aplicações da organização de todos os outros dados e aplicações no dispositivo móvel (Solução MDM)	network		x			
					• Realização de avaliação de risco para cada aplicação de terceiros antes de permitir a utilização nos dispositivos móveis da organização.	si	x		existe		

A = Aplicável; NA = Não aplicável

Tabela 4.9 - Modelo de posicionamento ICT (MPICT)

Conforme descrito nas notas das instruções de preenchimento oferecem-se alguns campos de validação que podem ser visualizados no exemplo disponível no Anexo E ou na ferramenta.

Foi igualmente desenvolvida a possibilidade de obter uma visão gráfica do posicionamento versus impacto no negócio e do esforço de implementação conforme demonstrado na Figura 4.2, produzidos com valores fictícios como forma de testar o modelo proposto. Esta visão pode ser igualmente útil no suporte à tomada de decisão pelo que podem ser integrados no modelo seguinte.

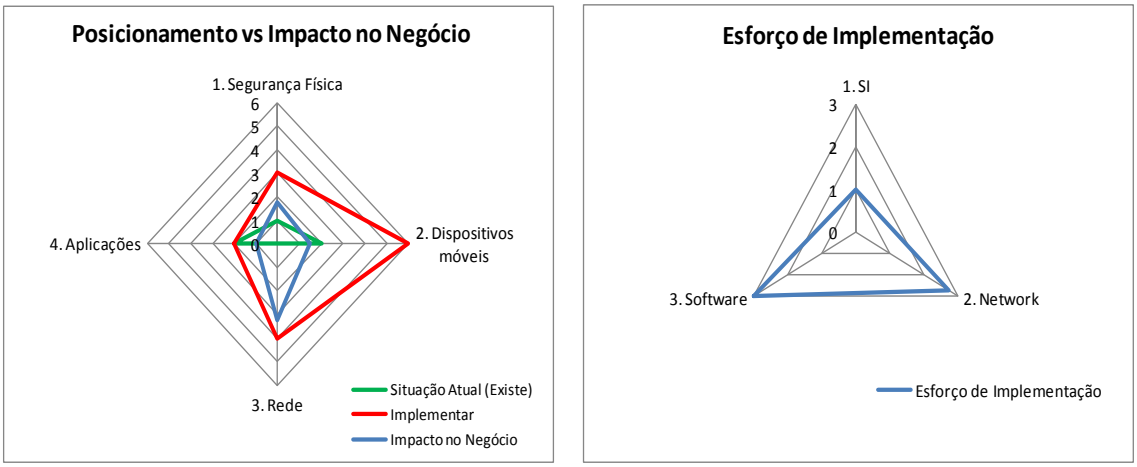

Figura 4.3 - Gráficos exemplificativos baseados no modelo de posicionamento proposto

Ao estabelecer os diferentes cenários de ameaça e os possíveis controlos de segurança e/ou medidas de mitigação necessárias, tendo em conta as soluções que já existem na organização e as que são necessárias implementar, é possível obter a visão do posicionamento ICT em relação à adoção da solução BYOD.

A recolha da informação do posicionamento ICT vai igualmente possibilitar a entrega de *inputs* para a análise seguinte, ou seja para a análise custo-benefício.

4.4 Modelo de Análise Custo-Benefício (MCBA)

O objetivo deste modelo é estabelecer a análise de custo versus benefício da implementação da solução BYOD. No Anexo F, baseado no Capítulo 3, é apresentada uma lista de fatores e aspetos a considerar na implementação de soluções BYOD. Foram consideradas as áreas: "1.Produtividade", "2.Dispositivos" e "3.Telecomunicações" como representativos de potenciais ganhos e as áreas: "4.Infraestrutura", "5.Aplicações corporativas", "6.Suporte e formação" como potenciais custos.

Em termos de "1. Produtividade" é necessário identificar os fatores a utilizar na medição da produtividade. Em primeiro lugar é preciso definir a unidade de medida (monetária, por exemplo em relação ao montante auferido; ou quantitativa, como por exemplo o número de bens produzidos, de chamadas atendidas, de serviços contratados, etc.). De seguida, medir a produtividade no espaço temporal, podendo ser uma hora, um dia, uma semana, um mês, etc. O passo seguinte é estabelecer o resultado do trabalho através da recolha dos resultados (unidade de medida por espaço temporal) de vários colaboradores e depois calcular o tempo de trabalho efetivo despendido para a realização das tarefas em questão. A produtividade pode ser calculada considerando os resultados obtidos durante o período de tempo definido, dividido pelo número de horas de trabalho gasto. No caso de existir um grupo de colaboradores piloto da implementação da solução BYOD podem ser aplicadas as medidas anteriores e comparado os resultados. Outro método possível consiste em avaliar a predisposição dos colaboradores quanto à solução BYOD, através de *surveys*. Com base nas respostas pode ser extrapolado a maturidade dos colaboradores e a predisposição dos mesmos para a adesão de soluções BYOD transformando valores intangíveis, como a iniciativa, ou o aumento da satisfação e motivação dos colaborares em valores tangíveis.

Para cálculo de "2.Dispositivos" dependem diversos fatores. A ideia inicial é que o custo do dispositivo é transferido de imediato para o colaborador, no entanto é necessário ponderar outros fatores, como por exemplo o valor da amortização do dispositivo, a perda de descontos obtidos com a compra massiva de dispositivos por parte da organização (para o caso de só uma parte da organização aderir à solução BYOD) ou a substituição do dispositivo pelo colaborador em caso de perda ou roubo versus o tempo de substituição (inoperacionalidade do colaborador durante esse período). Esta situação pode ser obtida considerando por exemplo os atuais valores referentes às comunicações de perda ou roubo de dispositivos corporativos. Ponderando que o colaborador pode não ter disponibilidade imediata de substituir o seu dispositivo, há que considerar a necessidade de existirem ou não dispositivos de reserva (depende sobretudo do tipo de dispositivo envolvido, exemplo dos *laptops*) e do tipo de aplicações corporativas que são acedidas via esse dispositivo (exemplo, se trata-se de colaboradores que dão suporte a aplicações criticas ou simplesmente a aplicações de consulta com menor impacto).

Em termos da análise "3.Telecomunicações", há que considerar sobretudo os planos/pacotes de voz e dados. Caso seja da responsabilidade da organização há que

avaliar se o plano é suficiente (por exemplo se incorpora dados e a sua limitação). No caso de transferirem o custo do plano/pacotes para os colaboradores BYOD se implica perda dos descontos atuais (tendo em conta por exemplo que só um grupo de colaboradores adere à solução BYOD).

Na Tabela 4.10 é proposto o modelo de análise custo-benefício (MCBA) referente aos potenciais benefícios. Os valores utilizados neste exemplo são fictícios e devem ser estimados/calculados para aplicação do modelo.

Não sendo o âmbito desta dissertação a análise específica de uma organização, considerou-se (e não havendo dados mais recentes) o estudo realizado pela Cisco IBSG (2013) em 2013 referente aos dados sobre produtividade, dispositivos móveis e telecomunicações. O estudo revela que em termos globais 36% dos colaboradores BYOD economizam pelo menos duas horas por semana (estabelecendo-se esta percentagem como objetivo a atingir) e 21% economizam pelo menos quatro horas por semana (objetivo mínimo de colaboradores), O estudo concluiu igualmente que a média dos colaboradores BYOD economizam cerca de 37 minutos por semana traduzindo-se num ganho anual de 350 dólares (atualmente cerca de 331,52 euros) anuais por colaborador móvel.

Em relação aos dispositivos móveis e tendo como referência o mesmo estudo, 81% utilizam *smartphones* pessoais, 56% recorrem a *tablets* e 37% utilizam *laptops* pessoais no desempenho das suas funções, pelo que considerou-se estas percentagens como referência em termos de objetivos.

Relativamente às telecomunicações o estudo revela que vinte por cento dos colaboradores migraram de planos corporativos para planos individuais.

As percentagens consideradas são meramente exemplos, sendo que as organizações devem estabelecer os seus valores. Para o exercício estabeleceu-se uma organização com 300 colaboradores e aplicou-se as percentagens referidas no estudo da Cisco (2013). O valor relativo à diminuição dos custos foi efetuado considerando a extrapolação do tempo economizado anualmente por colaborador multiplicado quantidade de colaboradores BYOD mais o dinheiro economizado a partir do custo real dos dispositivos e do custo do plano de telecomunicações a transferir para o colaborador.

Considerou-se valores dos dispositivos móveis e de telecomunicações sem ter sido realizada uma pesquisa de mercado aprofundada, sendo os valores apresentados meramente exemplificativos.

Instruções de Preenchimento:
Passo 1*: identificar e documentar os fatores a utilizar na medição da produtividade, extrapolando o tempo economizado. Proceder da mesma forma para a área dos dispositivos e telecomunicações.*
Notas: *Adicionalmente identificar a quantidade de colaboradores BYOD atual e/ouestimada.*
Os benefícios são calculados automaticamente na coluna "Total".
O total dos benefícios são calculados automaticamente considerando o critério: (tempo economizado x valor base do salário médio da organização) + dinheiro economizado a partir do custo real do dispositivo + custo do plano de telecomunicações.

Áreas	Fatores	Base de Cálculo	Referência (1)		Valores Macro		TOTAL
			Min.	Goal			
1.Produtividade	Satisfação	tempo economizado anualmente	21% (1)	36% (1)	# colaboradores - (universo: 36% em 300)	108	35,804 €
	Flexibilidade						
	Iniciativa				tempo economizado anualmente por colaborador (euros) (1)	331.52 €	
2.Dispositivos	Compra dos dispositivos	dinheiro economizado a partir do custo real do dispositivo		(1) 81% smartphones 56% tablets 37% laptops	# colaboradores - *smartphones* (universo: 81% em 300)	243	317,846 €
					custo real do dispositivo - *smartphones* (euros)	599.99 €	
	Substituições dos dispositivos				# colaboradores - *laptopts* (universo: 37% em 300)	111	
					custo real do dispositivo - *laptops* (euros)	1,549.99 €	
3.Telecomunicações	Planos de voz e dados	custo do plano de telecomunicações.		20%	# colaboradores (universo: 20% em 300)	60	1,826.40 €
					custo do plano de telecomunicações (euros) (2)	30.44 €	
Total de Benefícios		tempo economizado anualmente + dinheiro economizado a partir do custo real do dispositivo + custo do plano de telecomunicações.					**355,477 €**

Notas:
(1) Cisco ISBG (2013).
(2) http://negocios.vodafone.pt/tarifarios/red-biz.html

Tabela 4.10 - Modelo de análise custo-benefício (MCBA) – Potenciais Benefícios

Para os fatores identificados em “4.Infraestrutura”, “5.Aplicações corporativas” e “6.Suporte e formação” foi efetuado o relacionamento com o modelo de posicionamento ICT, considerando os pareceres ICT quanto à existência e/ou necessidade de alterações.

É necessário realçar que dependendo das organizações os fatores e variáveis de análise podem diferir. Alguns dos controlos de segurança e/ou medidas de mitigação podem também ser agrupados na mesma solução (exemplo das soluções MDM que incorporam controlos e/ou medidas abrangentes como a aplicação de políticas corporativas; a possibilidade do estabelecimento de espaços / *container's* criptografados para os dados corporativos nos dispositivos móveis; a gestão aplicacional corporativa e gestão de *backup*; a limpeza remota e a capacidade de restaurar dados) levando à diminuição de potenciais custos uma vez que engloba vários controlos e/ou medidas de mitigação. O importante é identificar todos os fatores, relacionar os diversos cenários e quantificar os valores na mesma medida unitária.

Na Tabela 4.11 é proposto o modelo de análise custo-benefício (MCBA) referente aos potenciais custos. Os valores utilizados neste exemplo são fictícios e devem ser estimados/calculados para aplicação do modelo.

Uma vez mais, e não estando no âmbito desta dissertação a análise específica de uma organização, estabeleceram-se custos monetários fictícios por controlo e/ou medida de mitigação com o objetivo de exemplificar a tabela e sem qualquer análise aprofundada dos valores de mercado.

Instruções de Preenchimento:
Passo 1: *Estabelecer o custo das soluções.*
Notas: *Os custos são calculados automaticamente na coluna "Total".*
O total dos benefícios são calculados automaticamente.

Áreas	Fatores	Mapeamento Posicionamento ICT		
		Controlos de Segurança e ou Medidas de Mitigação	**Recomendação ICT**	**TOTAL (k)**
4.Infraestrutura	Soluções MDM	• Limpeza *(wipe)* remoto (Solução MDM)	implementar	70,000 €
	Soluções Cloud	• Serviços de *Cloud Computing*	existe	€
	Network	• Soluções NAC (Network Access Control) ou EVA (Endpoint Visibility, Access, and Security);	na	€
		• Redes separadas (rede própria para dispositivos externos, em vez de acederem diretamente à rede interna)	implementar	50,000 €
		• Criptografia forte (como redes privadas virtuais, VPNs)	implementar	50,000 €
		• Mecanismos de autenticação mútua (verificação da identidade em ambos os *endpoints*) (Solução NAC ou EVA)	implementar	€
		• Desativação de interfaces de rede desnecessários	implementar	7,000 €
		• Implementação de *sandbox's/containers seguros* que isola os dados e as aplicações da organização de todos os outros dados e aplicações no dispositivo móvel (Solução MDM)	na	€
5.Aplicações corporativas	Desenvolvimento de aplicações corporativas	• Autenticação forte	na	€
		• Autenticação multi-fator	implementar	45,000 €
		• Cifrar o dispositivo ou os dados sensíveis	existe	€
		• Tecnologias *antimalware*: *software* antivírus, *firewalls* e *passwords*	implementar	30,000 €
		• Aplicações de análise da integridade dos dispositivos	na	€
	Licenciamento Software	• Disponibilização de software e, ou serviços por assinatura (exemplo: SAAS, Office 365, etc.)	implementar	50,000 €
6.Suporte e Formação	Politica BYOD	• Restrição dos dispositivos móveis, versões e sistemas operativos com controlo efetivo	implementar	800 €
		• Restrição e ou proibição do uso de determinadas aplicações	existe	€
		• Proibição do acesso a redes Wi-Fi inseguras, i.e., que executam protocolos com vulnerabilidades conhecidas	implementar	800 €
		• Disponibilização do mínimo (acessos) necessário	existe	€
		• Proibição da instalação de aplicações de terceiros	implementar	800 €
		• Criação de *whitelisting* das aplicações aprovadas	implementar	800 €
		• Realização de avaliação de risco para cada aplicação de terceiros antes de permitir a utilização nos dispositivos móveis da organização.	existe	€
	Programas de *awareness*	• Formação e *Awareness* (roubo e perda)	implementar	500 €
		• Formação e *Awareness* (sincronização entre dispositivos)	implementar	500 €
	Suporte *help-desk*	• Formação e *Awareness* (licenciamento)	implementar	500 €
Custos Totais				**306,700 €**

Tabela 4.11 - Modelo de análise custo-benefício (MCBA) – Potenciais Custos

A diferença entre os valores obtidos na Tabela 4.10 e na Tabela 4.11, ou seja, a diferença entre o resultado final dos benefícios e o resultado final dos custos vai permitir avaliar o impacto financeiro da implementação da solução BYOD.

Na Tabela 4.12 é apresentado o modelo de decisão simples baseado no CBA (MCBA) onde estão presentes os totais por áreas e onde são subtraídos aos benefícios totais, os custos totais. Foi disponibilizado igualmente uma área para resumo da análise.

MCBA	Áreas	Fatores Macro	Cálculo	TOTAL (k)
Benefícios	**1.Produtividade**	Satisfação	tempo economizado anualmente	35,804 €
		Flexibilidade		
		Iniciativa		
	2.Dispositivos	Compra dos dispositivos	dinheiro economizado a partir do custo real do dispositivo	317,846 €
		Substituições dos dispositivos		
	3.Telecomunicações	Planos de voz e dados	custo do plano de telecomunicações	1,826 €
BENEFÍCIOS TOTAIS				**355,477 €**
Custos	**4.Infraestrutura**	Soluções MDM	∑ Custos (€)	177,000 €
		Soluções Cloud		
		Network		
	5.Aplicações corporativas	Desenvolvimento de aplicações corporativas	∑ Custos (€)	125,000 €
		Licenciamento Software		
	6.Suporte e Formação	Politica BYOD	∑ Custos (€)	4,700 €
		Programas de awareness		
		Suporte help-desk		
CUSTOS TOTAIS				**306,700 €**
Fórmula CBA = Benefícios – Custos				**48,777 €**

Custos inferiores aos benefícios

A análise efetuada demonstra que os benefícios (355,477 €) de uma solução BYOD são superiores aos custos (306,700 €) da mesma pelo que a decisão de implementação da solução BYOD é favorável.

Custos superiores aos benefícios

Custos superiores aos benefícios no entanto verificou-se que:

- a % de colaboradores BYOD é alta (x%)
- a % de colaboradores BYOD tende a aumentar em X % no próximo ano
- tendência significativa do mercado para a adesão BYOD
- outra situação (especificar):

Tabela 4.12 - Modelo de decisão CBA (MCBA)

Assim, se na tabela de aplicação do MCBA os custos demonstrarem ser inferiores aos benefícios a implementação de uma solução BYOD é favorável; se os custos forem superiores aos benefícios tudo indica que a solução terá um impacto financeiro que não é acompanhado em termos de benefícios no entanto é necessário estar alerta para outras variáveis que possam condicionar a decisão como, por exemplo, a percentagem de

colaboradores BYOD na organização ou a tendência do mercado que pode justificar a necessidade de proteger os ativos da organização através da implementação de soluções BYOD.

4.5 Modelo *Checklist* da Política de Segurança BYOD (MCPSB)

Considerando um parecer favorável á implementação da solução BYOD é necessário definir regras sobre a utilização dos dispositivos móveis no contexto da organização. A infinidade de dispositivos pessoais pode ser complicada de gerir. Dependendo das opções pessoais verifica-se não só uma quantidade de dispositivos (*smartphones*, *tablets*, *laptops*, etc.) como também uma variedade de sistemas operativos (*iOS*, *Windows*, *Android*, etc.) e *software* (aplicações).

A política de segurança BYOD (Nunoo, 2013; Lydon, 2014; Agudelo et al., 2015) vai permitir informar os colaboradores das regras que a empresa adotou ou que pretende adotar com a implementação de uma solução BYOD.

A política de segurança BYOD é um documento que deve ter o apoio hierárquico da organização uma vez que envolve não só a camada estratégica como a operacional (Costa, 2015). Deve ser periodicamente revisto e atualizado tendo em conta o surgimento constante de novas ameaças.

A definição de uma Política de Segurança BYOD é específica à utilização dos dispositivos móveis no contexto da organização, pelo que deve ser dirigida a esse universo, devendo no entanto ressalvar as questões definidas em outros documentos de segurança, nomeadamente a necessidade em cumprir com outros procedimentos, como por exemplo os descritos na Política de Segurança em vigor, caso exista.

Na Tabela 4.13 é disponibilizado um modelo de suporte da Política de Segurança BYOD.

O modelo está agrupado em sete temas principais, estando descritos os tópicos que podem ser desenvolvidos. Este modelo pode constituir por si só uma ação de *awarness*, uma vez que permite instruir os colaboradores quanto a procedimentos e preocupações de segurança a adotar com a utilização dos dispositivos móveis.

1. Geral
1.1 Registar e definir as revisões periódicas da Política de Segurança de Dispositivos Móveis;
2. Definição de Responsabilidades
2.1 Quanto ao dispositivo – relacionado com questões de elegibilidade e de aceitação (a quem, o quê, onde, quando, e em que condições); **2.1.1** Quem - Definição das áreas ou departamentos que podem utilizar dispositivos móveis em contexto corporativo; **2.1.2** O Quê - Definição dos sistemas / aplicações disponíveis de acesso com os dispositivos móveis, considerando por exemplo a classificação dos dados que são acedidos; **2.1.3** Onde - Situações em que podem utilizar os dispositivos móveis e quais as medidas adicionais de segurança em locais fora da organização; **2.1.4** Quando - Definição por exemplo de programas de consciencialização da segurança móvel através de ações de *awarness* específica sobre comportamentos e utilização dos dispositivos móveis no contexto empresarial; **2.1.5** Em que condições - Identificação do método de consentimento formal do colaborador; **2.2** Quanto ao suporte prestado – nomeadamente: **2.2.1** Suporte ICT prestado pela organização (exemplo para questões de conectividade às aplicações corporativas); **2.2.2** Suporte prestado por fornecedores do dispositivo (exemplo para questões relacionadas com o hardware);
3. Definição dos Dispositivos móveis permitidos
3.1 Identificação dos dispositivos permitidos (exemplo: *smartphones*, *tablets*, *personnal computers*, etc); **3.1.1** Tipo de dispositivos; **3.1.2** Análise de confiabilidade; **3.2** Sistemas operativos e versões (segundo parecer ICT no que respeita a requisitos de segurança);
4. Definição dos Procedimentos de Gestão, Configuração e Segurança dos Dispositivos
4.1 Definição da(s) solução(ões) de gestão de dispositivos móveis (software MDM); **4.2** Procedimentos de monitorização e controlo dos dispositivos móveis, como por exemplo, a possibilidade de limpezas (*wipe*) remotas, em que situações (exemplo, através das soluções MDM); **4.3** Necessidade de instalação de *container's ("sandboxs")* nos equipamentos que permitam separar os dados corporativos dos dados privados do colaborador; **4.4** Definição dos métodos de autenticação (por exemplo, utilização do procedimento descrito na Política de Segurança, caso exista, quanto à configuração das passwords, nomeadamente robustez, tamanho, histórico, etc.) e face à classificação de dados que são acedidos via dispositivos móveis; **4.5** Definição dos protocolos e métodos de cifra utilizados/necessários, tendo em conta o manuseamento (acesso / transmissão / transporte) do tipo de informação com os dispositivos;
5. Definição dos Procedimentos de Ativação e Desativação dos Dispositivos Móveis
5.1 Procedimento de ativação do dispositivo na rede corporativa (como por exemplo: agendar com a área de ICT a configuração; inscrição em site online, instalação de software MDM, outra situação); **5.2** Necessidade de precauções adicionais, nomeadamente quanto à salvaguarda / cópia de segurança dos dados (backups), transporte, etc. **5.3** Procedimento de desativação do dispositivo, por exemplo: **5.3.1** Por roubo/perda dos equipamentos – tempo em que deve ser reportado, forma de reportar (por exemplo de forma online, possibilidade do próprio em desativar o dispositivo; etc.); **5.3.2** Por saída do colaborador; **5.3.3** Por comprometimento do dispositivo - identificação de incidentes de segurança;
6. Definição do Procedimentos de "Utilização Aceitável"
6.1 Identificação das aplicações: **6.1.1** Lista de aplicações permitidas; **6.2.2** Lista de aplicações proibidas (exemplo aplicações que não estejam disponíveis via iTunes ou Google Play); **6.2.3** Lista dos recursos corporativos disponíveis (como por exemplo, email, calendário, sites web corporativos, aplicações corporativas disponíveis); **6.2** Utilização do dispositivo durante o período laboral, no que respeita à utilização de jogos e, ou tempo despendido em redes sociais;
7. Definição do Procedimento quanto ao não cumprimento da política
7.1 Definição do não cumprimento; **7.2** Sanções por não cumprimento - exemplo negação do acesso à rede corporativa, exclusão do colaborador da solução BYOD, aplicação de ação disciplinar.

Tabela 4.13 - Modelo *Checklist* da Política de Segurança BYOD

4.6 Avaliação do modelo proposto

Com o intuito de avaliar o modelo proposto foi disponibilizado um questionário através do link:

https://www.survio.com/survey/d/W8E1T3P2N9N4G6M6I#.WJSTumjg8xY.google_plusone_share.

4.7 Resumo

O modelo proposto neste trabalho tem como intuito apresentar diferentes modelos de dados sejam eles de cariz legal, operacional ou financeiro, imprescindíveis no suporte à decisão de soluções BYOD.

Os fatores apresentados não devem ser encaradas como fatores fixos e universais. A decisão e avaliação dos fatores devem ser as adequadas e dependem dos objetivos que cada organização pretende atingir.

Não obstante, o modelo proposto é constituído por cinco modelos independentes que no final constituem uma ferramenta de avaliação da solução BYOD. Assim temos os modelos que se sumariam de seguida.

O Modelo de análise dos Requisitos Legais Obrigatórios (MRLO) permite assinalar e priorizar as questões legais face aos valores monetários (sanções ou coimas).

O Modelo de Avaliação dos Riscos (MAR) permite uma análise dos ativos; estabelecer a criticidade dos mesmos baseado nas potenciais ameaças; definir ou excluir ativos; limitar a solução BYOD a determinados dispositivos móveis, áreas ou grupo de colaboradores da organização; e identificar o nível de risco dos ativos expostos à solução BYOD.

O Modelo de Posicionamento ICT (MPICT) permite estabelecer a posição da organização em relação à implementação da solução BYOD através da identificação dos cenários de ameaças; dos controlos de segurança e/ou medidas de mitigação; dos mecanismos já existentes; dos que serão necessárias implementar e dos custos relacionado com esforços de implementação.

O Modelo Análise Custo-Benefício (MCBA) permite finalizar a decisão quanto à implementação da solução BYOD. O modelo assim como os fatores diferem de organização para organização, sendo importante alinhar a análise com os objetivos das mesmas. Do mesmo modo os custos e os benefícios podem igualmente diferirem.

O Modelo *checklist* da Política de Segurança BYOD (MCPS) pretende modelar a elaboração e apresentação de política de segurança BYOD na organização. Depende sobretudo da decisão de implementação e do modelo escolhido para a solução BYOD.

Capítulo 5

Conclusão

5.1 Discussão

As soluções BYOD surgem como uma tendência emergente na área de ICT, revolucionando a forma de trabalho das organizações. Sendo quase impossível de travar, não só pelo mercado consumista em que vivemos, mas também pela evolução da tecnologia, o BYOD representa uma nova era em ICT – tecnologias móveis, serviços de *Cloud Computing*, *Big Data Solutions* (soluções de análise de dados complexos e em grande escala), diversidade de aplicações sociais, IoT (*Internet of Things*), etc.

O BYOD implica desafios para os profissionais da segurança da informação, no que concerne à segurança da informação – confidencialidade, privacidade e integridade; mas também preocupações em termos legais – proteção de dados sensíveis, evasão de privacidade, regulação e legislação aplicável.

Apesar dos objetivos da solução BYOD poderem ser definidos de início há que avaliar objetivamente o sucesso da solução. Desta forma é necessário estabelecer o conjunto de variáveis que vão permitir decidir a viabilidade do projeto, tendo em conta que as variáveis podem sofrer alterações ao longo da análise.

O sucesso da solução BYOD está diretamente relacionado com o envolvimento e os esforços da organização nomeadamente de áreas de ICT, dos recursos humanos, da área jurídica, mas também e principalmente com a predisposição e comportamento dos colaboradores em relação à solução.

Durante a elaboração do trabalho foram adquiridos conhecimentos e aprendidas algumas lições, como por exemplo a necessidade em apostar fortemente numa cultura da segurança da informação. A conscientização da segurança da informação é deveras importante e deve ser incutida e estar presente nas pessoas, nos processos e não só através da tecnologia. Ser conhecedor das ameaças, dos riscos e dos métodos que

efetivamente podem ser usados como defesa, é essencial para o sucesso de projetos assentes principalmente em comportamentos individuais, como é o caso da solução BYOD.

5.2 Trabalho Futuro

O modelo proposto nesta dissertação pode ser utilizado pelas organizações para suporte à decisão de avaliação da implementação da solução BYOD.

De salientar que quer as variáveis quer as opções feitas foram sendo estabelecidas de forma a testar o modelo pelo que, outras variáveis ou opções podem ser consideradas sendo que certamente conduzirão a resultados diferentes dos que foram apresentados neste trabalho.

Como trabalho futuro em termos de modelo sugere-se a especificação de submodelos de suporte ao modelo de análise custo-benefício consoante as diferentes possibilidades de análise. Em termos de ferramenta sugere-se a possibilidade de automatizar a mesma, criando-se uma folha com a informação principal onde os modelos seguintes recorrem para a construção da restante análise, aplicando-se as variáveis definidas inicialmente; ou mesmo o desenvolvimento em WEB sendo mais apelativo no que respeita à apresentação de resultados.

Por último recomenda-se a implementação do modelo proposto numa organização com o objetivo de validar o mesmo e identificar possibilidades de melhoria.

Como em qualquer outro projeto os modelos, os fatores, e os controlos escolhidos devem ser avaliados, testados e melhorados de acordo com os resultados obtidos. Nesse sentido foi elaborado um questionário de avaliação ao modelo proposto e disponibilizado através do link:

https://www.survio.com/survey/d/W8E1T3P2N9N4G6M6I#.WJSTumjg8xY.google_plusone_share.

Perspetiva-se a recolha e análise de respostas a este questionário para futuras iterações de desenvolvimento do modelo que esta dissertação propõe.

Bibliografia

Agudelo, C.A., Bosua, R., Ahmad, A., Maynard, S.B., 2015. *Understanding Knowledge Leakage & BYOD (Bring Your Own Device): A Mobile Worker Perspective*. Australasian Conference on Information Systems, 2015. Disponível *online*: https://arxiv.org/abs/1606.01450. Último acesso: Julho 2016.

Arregui, D.,2015.*Mitigating BYOD information security risks*. Minor Research Project in IS in the University of Melbourne, novembro 2015. Disponível *online*: http://hdl.handle.net/11343/56627. Último acesso: Setembro 2015.

Caralli, R.A., Stevens, J.F., Young, L.R., Wilson, W.R., 2007. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.*Carnegie Mellon University, maio 2007. Disponível *online*: http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8419. Último acesso: Setembro 2015.

CESG, 2015. *Analysis of information risk management methodologies*. UK Government's National Technical Authority for Information Assurance (CESG), março 2015. Disponível *online*: https://www.gov.uk/guidance/analysis-of-information-risk-management-methodologies#more-like-this. Último acesso: Junho 2015.

Cisco IBSG, 2013. *The Financial Impact of BYOD*. Cisco IBSG, 2013. Disponível *online*: https://www.cisco.com/web/about/ac79/docs/re/byod/BYOD-Economics_Econ_Analysis.pdf. Último acesso: Junho 2015.

Cisco, 2014. *Cisco Unified Access (UA) and Bring Your Own Device (BYOD) CVD.* Cisco Systems, Inc., agosto 2014. Disponível *online*: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide.html. Último acesso: Junho 2015.

Computer Weekly, 2012. *The cost and benefits of BYOD*. ComputerWeekly, junho 2012. Disponível em:

http://www.computerweekly.com/news/2240158445/Forrester-The-costs-and-benefits-of-BYOD. Ultimo acesso: Setembro 2015.

Costa, M., O., 2015. *BYOD: bring your own device in Portugal*. Globe Business Media Group, junho 2015. Disponível online: http://www.lexology.com/library/detail.aspx?g=815e46a1-1644-47dc-88e0-3369dfd2dd19. Último acesso: Julho 2016.

ENISA, 2006. *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools*. European Union Agency for Network and Information Security (ENISA), junho 2006. Disponível *online*: http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-ra-methods. Último acesso: Junho 2015.

ENISA, 2015. *Risk Management*. European Union Agency for Network and Information Security (ENISA), 2005-2015. Disponível *online*: https://www.enisa.europa.eu/activities/risk-management. Último acesso: Junho 2015.

Finneran, M., & Brashear,J.,2014. *A legal prespective of BYOD.* ZIXCorp, janeiro 2014. Disponível *online*: http://blog.zixcorp.com/2014/02/ebook-snapshot-a-legal-perspective-of-byod/. Último acesso: Junho 2015.

Fonseca, P., 2014. *Organizações nacionais pouco receptivas ao BYOD.* ComputerWorld, abril 2014. Disponível *online*: http://www.computerworld.com.pt/2014/04/23/organizacoes-nacionais-pouco-receptivas-ao-byod/. Último acesso: Junho 2015.

Forrester Research, Inc., 2012. *Key Strategies To Capture And Measure The Value Of Consumerization Of IT*. Forrester Research, Inc., maio 2012. Disponível *online*: http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_forrester_measure-value-of-consumerization.pdf. Último acesso: Junho 2015.

Gilmore, G. & Beardmore. P., 2013. *Mobile Security & BYOD For Dummies*.John Wiley & Sons, Ltd.,2013.

IDC Portugal, 2015. *Estudo sobre as principais tendências tecnológicas em Portugal - Mobilidade: Como Criar valor para o seu negócio?*.IDC Tech insights 2020, 2015. Disponível *online*: http://www.cvent.com/events/portugal-tech-insights-2020-idc-nos/event-summary-972d971428814a96997bcd5a1c7eb6e2.aspx. Último acesso: Julho 2016.

InfoLawGroup, 2012. *The Security, Privacy and Legal Implications of BYOD (Bring Your Own Device).* InfoLawGroup LLP, março 2012. Disponível *online*: http://www.infolawgroup.com/2012/03/articles/byod/the-security-privacy-and-legal-implications-of-byod-bring-your-own-device/. Último acesso: Junho 2015.

Investopedia, 2015a. *IRR- Internal Rate of Return.*Investopedia, LLC, 2015. Disponível *online*: http://www.investopedia.com/terms/i/irr.asp?optm=term_v3. Último acesso: Junho 2015.

Investopedia, 2015b. *NPV- Net Present Value*. Investopedia, LLC, 2015. Disponível *online*: http://www.investopedia.com/terms/n/npv.asp?optm=sa_v1. Último acesso: Junho 2015.

ISACA, 2009. *The Risk IT Framework.*ISACA, 2009. Disponível *online*: http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fmk_Eng_0109.pdf. Último acesso: Junho 2015.

ISACA, 2012a. *COBIT 5 Introduction - Isaca*. ISACA, 2012. Disponível *online*: https://www.isaca.org/COBIT/Documents/COBIT5-Introduction.ppt. Último acesso: Junho 2015.

ISACA, 2012b. *COBIT 5 A Business Framework for the Governance and Management of Enterprise IT*. ISACA, 2012. Disponível *online*: http://www.isaca.org/cobit/Pages/CobitFramework.aspx. Último acesso: Junho 2015.

ISACA, 2013. *COBIT® 5 for Risk Introduction*. ISACA, 2013. Disponível *online*: http://www.isaca.org/cobit/pages/cobit-5-implementation-product-page.aspx. Último acesso: Junho 2015.

ISACA, 2015. *About ISACA.* ISACA, 2015. Disponível *online*: http://www.isaca.org/About-ISACA/Press-room/Documents/2015-ISACA-Fact-Sheet_pre_eng_0715.pdf. Último acesso: Junho 2015.

ISO, 2013. *NP ISO 31000:2013 Gestão do Risco – Princípios e linhas de orientação (ISO 31000:2009)*, IPQ, Portugal.

ISO/IEC, 2011. *ISO/IEC 27005:2011 – Information technology – Security techniques – Information security risk management, 2nd Edition*, International Organization for Standardization, Switzerland.

ISO/IEC, 2013. *NP ISO/IEC 27001:2013 Tecnologia de informação – Técnicas de segurança, Sistemas de gestão de segurança da informação - Requisitos*, IPQ, Portugal.

Jones, J.A., 2005. *An Introduction to Factor Analysis of Information Risk (FAIR)*. Risk Management Insight LLC, 2005. Disponível *online*: http://riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf. Último acesso: Junho 2015.

Keyes, J., 2013. *Bring Your Own Devices (BYOD) Survival Guide*. Taylor & Francis Group, LLC.

KPMG, 2013. *Gestão do Risco em Portugal: Desafios para as Empresas*. KPMG Advisory - Consultores de Gestão, S.A., maio 2013. Disponível *online*: https://www.kpmg.com/PT/pt/IssuesAndInsights/Documents/surveyERM2013.pdf. Último acesso: Junho 2015.

Lydon, E., 2014. *The Benefits and Threats of BYOD in a SME Enterprise. A Systematic Literature Review*.Master of Science in Information Security in the Luleå University of Technology, 2014. Disponível *online*: http://pure.ltu.se/portal/en/studentthesis/the-benefits-and-threats-of-byod-in-a-sme-enterprise(6472b6da-c088-4d52-b2ac-9dbadd78f4cc).html. Último acesso: Setembro 2015.

Mamede, H.S., 2006. *Segurança Informática nas Organizações.*FCA-Editora de Informática,Lda.

Marinos, L., 2014. *Overview of current and emerging cyber-threats*. ENISA Threat Landscape, 2014. Disponível *online*: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014. Último acesso: Junho 2015.

Mavretich,R.J., 2012. *Legal Issues within Corporate "Bring Your Own Device" Programs.* SANS Institute, maio 2012. Disponível *online*: https://www.sans.org/reading-room/whitepapers/legal/legal-issues-corporate-bring-device-programs-34060. Último acesso: Junho 2015.

Mitre, 2014. *Systems Engineering Guide.* The MITRE Corporation, 2014. Disponível online: https://www.mitre.org/sites/default/files/publications/se-guide-book-interactive.pdf. Último acesso: Junho 2015.

NIST, 1996. *Generally Accepted Principles and Practices for Securing Information Technology Systems*. National Institute of Standards and Technology (NIST), setembro 1996. Disponível *online:* http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf. Último acesso: Junho 2015.

NIST, 2008. *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*. National Institute of Standards and Technology (NIST), agosto 2008. Disponível *online:* http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf. Último acesso: Junho 2015.

NIST, 2012. *Guide for Conducting Risk Assessments*. National Institute of Standards and Technology (NIST), setembro 2012. Disponível *online:* http://www.nist.gov/customcf/get_pdf.cfm?pub_id=912091. Último acesso: Junho 2015.

NIST, 2013. *Guidelines for Managing the Security of Mobile Devices in the Enterprise*. National Institute of Standards and Technology (NIST), junho 2013. Disponível *online:* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf. Último acesso: Junho 2015.

Nucleus Research, N65, 2013.*Understanding the hard ROI of BYOD*. Nucleus Research, Inc., abril 2013. Disponível *online*: https://nucleusresearch.com/download/n65-understanding-the-hard-roi-of-byod-1404-pdf/. Ultimo acesso: Junho 2015.

Nunoo, E. M., 2013. *Smartphone Information Security Risks, Portable Devices and Workforce Mobility*. Master of Science in Information Security in the Luleå University of Technology, 2013. Disponível *online:* http://ltu.diva-portal.org/smash/record.jsf?pid=diva2%3A1019739&dswid=-5586. Ultimo acesso: Setembro 2015.

Panda, P., 2009. *The OCTAVE® Approach to Information Security Risk Assessment*. ISACA Journal Volume 4, 2009. Disponível *online:* http://www.isaca.org/Journal/archives/2009/Volume-4/Documents/jpdf094-the-OCTAVE.pdf. Último acesso: Junho 2015.

Risk Management Insight, 2006. *FAIR (Factor Analysis of Information Risk), Basic Risk Assessment Guide.* Risk Management Insight, LLC., 2006. Disponível *online*: http://www.riskmanagementinsight.com/media/docs/FAIR_brag.pdf. Último acesso: Junho 2015.

Rivera, D., George, G., Peter, P., Muralidharan, S., & Khanum, S. 2013. *Analysis of security controls for BYOD (Bring Your Own Device)*.Research publication in the University of Melbourne, 2013. Disponível *online*: https://minerva-access.unimelb.edu.au/handle/11343/33338. Último acesso: Junho 2015.

Schulze, H., 2016. *BYOD & Mobile Security Report*. Crowd Research Partners, 2016. Disponível *online*: http://www.crowdresearchpartners.com/wp-content/uploads/2016/03/BYOD-and-Mobile-Security-Report-2016.pdf. Último acesso: Julho 2016.

The Open Group, 2009. *Technical Standard, Risk Taxonomy*. The Open Group, janeiro 2009. Disponível *online*: http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf. Último acesso: Junho 2015.

The Open Group, 2013. *Open Group Standard, Risk Taxonomy (O-RT), Version 2*. The Open Group, 2013. Disponível *online*: https://www2.opengroup.org/ogsys/catalog/C13K. Último acesso: Junho 2015.

Weber, L., 2014. *Addressing the incremental risks associated with adopting a Bring Your Own Device program by using the COBIT 5 framework to identify key controls.* Thesis for the degree of MCOMM (Computer Auditing) in the Faculty of Economic and Management Sciences School of Accounting at Stellenbosch University, abril 2014. Último acesso: Setembro 2015.

Whitman, M. E. & Mattord, H. J., 2010. *Management of Information Security*, 3rd Edition, Course Technology, Cengage Learning, 2010.

Legislação:

Código do Trabalho. Disponível *online*: http://www.cite.gov.pt/pt/legis/CodTrab_indice.html. Último acesso: Março 2016.

Lei 46/2012, de 29 de agosto. Diário da República n.º 167 – I Série de 29 de agosto de 2012. Disponível *online*: http://www.citius.mj.pt/portal/article.aspx?ArticleId=1208. Último acesso: Março 2016.

Lei 67/98, de 26 de outubro. Diário da República n.º 247 – I Série – A de 26 de Outubro de 1998. Disponível *online*: http://www.dgpj.mj.pt/DGPJ/sections/leis-da-justica/livro-iv-leis-criminais/pdf3/l-67-1998/downloadFile/file/L_67_1998.pdf?nocache=1181836313.44. Último acesso: Março 2016.

Lei 109/2009 de 15 de setembro. Diário da República n.º 166/2015 – I Série de 26 de agosto de 2015. Disponível *online*: https://dre.pt/application/file/70114275. Último acesso: Março 2016.

Anexo A – Resumo Metodologias de Análise e Avaliação de Risco

Nota: Os * representam o ênfase dado ao tema por determinada metodologia (* menor ênfase, ** ênfase médio, *** maior ênfase).

Metodologia	Proprietário	Objetivos	Método	Metodologia de Risco	Atividades	Avaliação do Risco			Tratamento do risco	Aceitação do Risco	Comunicação do Risco	Monitorização do Risco	Tipo de Organizações	Compatível	Disponibilidade
						Identificação	Análise	Avaliação							
COBIT 5	ISACA	Orientações em termos de estruturas de governação e gestão efetivas baseadas numa visão holística	Aborda requisitos de controlo, problemas técnicos e riscos de negócio	Quantitativa e qualitativa	5 Princípios 7 Facilitadores Guias Profissionais específicos - COBIT 5 for the risk	**	**	**	**			**	Aplicável a todo o tipo de organizações (foco nas questões de conformidade com requisitos legais e regulações externas)	ITIL,ISO/IEC, PMBOK, PRINCE2, TOGAF	not free
FAIR	Risk Management Insight LLC	Perceber, analisar e medir o risco da informação	Quantificar a informação e o risco operacional em termos financeiros	Quantitativa e qualitativa	4 Fases 10 Passos	**	**	***	**	**	*		Aplicável a todo o tipo de organizações	COSO, ITL, ISO/IEC, COBIT, OCTAVE, etc.	free

Metodologia	Proprietário	Objetivos	Método	Metodologia de Risco	Atividades	Avaliação do Risco			Tratamento do risco	Aceitação do Risco	Comunicação do Risco	Monitorização do Risco	Tipo de Organizações	Compatível	Disponibilidade
						Identificação	Análise	Avaliação							
ISO/IEC 27005	ISO/ IEC	Fornecer orientações para a gestão de riscos de segurança da informação	Suportar as orientações dos requisitos de criação, manutenção e de melhoria contínua dos SGSI	Qualitativa e quantitativa (inicialmente análise qualitativa, podendo particularizar os riscos principais em análises quantitativas)	7 Atividades ~30 Subactividades	**	**	**	***	***	***	***	Aplicável a todo o tipo de organizações	ISO/IEC 27001:2013	not free
SP800-30 (NIST)	NIST	Fornecer recomendações e orientações relacionadas com a segurança da informação	Visão de alto nível do processo de avaliação de risco	depende da ferramenta	4 Passos 15 Tarefas	**	**	**			**	**	Aplicável a todo o tipo de organizações (no entanto direcionada para organizações que seguem os padrões e regulações dos EUA)	ISO e outras metodologias	free
OCTAVE Method	SEI	Identificar e avaliar os riscos de segurança da informação	*Workshops* conduzidos por equipas de análise multidisciplinares (composta por elementos das diferentes unidades de negócio e de ICT)	Qualitativa e quantitativa (avaliação qualitativa podendo ser usada para análises quantitativas simples)	3 Fases 8 Processos	**	**		**	**	**		Direcionado para organizações grandes (> 300 colaboradores)		free

Metodologia	Proprietário	Objetivos	Método	Metodologia de Risco	Atividades	Avaliação do Risco			Tratamento do risco	Aceitação do Risco	Comunicação do Risco	Monitorização do Risco	Tipo de Organizações	Compatível	Disponibilidade
						Identificação	Análise	Avaliação							
OCTAVE-S	SEI	Identificar e avaliar os riscos de segurança da informação	Assume-se que existe o conhecimento prático dos ativos relacionados com informações importantes, requisitos de segurança, ameaças e práticas de segurança da organização	Qualitativa e quantitativa (avaliação qualitativa podendo ser usada para análises quantitativas simples)	4 Processos f Fases	**	**		**	**	**		Direcionado para organizações mais pequenas (<= 100 Colaboradores)		free
OCTAVE Allegro	SEI	Identificar e avaliar os riscos de segurança da informação	Recorre Workshops, colaboração e orientação no entanto sem ser necessário um grande envolvimento organizacional, experiência, ou conhecimentos iniciais- avaliação alargada dos riscos operacionais	Qualitativa e quantitativa (avaliação qualitativa podendo ser usada para análises quantitativas simples)	4 Fases 8 Processos	**	**		**	**	**	**	Aplicável a todo o tipo de organizações		free

Anexo B – Levantamento de informação para a implementação da solução BYOD

Âmbito	Grupo	Requisitos Legais obrigatórios	Possíveis soluções	Envolvimento das áreas		
Solução BYOD		**Modelo não previsto na legislação portuguesa aplicando-se *mutatis mutandis* ao BYOD (i.e., analogia ao que existe considerando as devidas proporções e alterações necessárias) (Costa, 2015).**		**Jurídico**	**ICT**	**RH**
Corporativos	**1. Proteção dos dados sensíveis corporativos**	Solução BYOD que considere: • Processamento de dados- obrigatório a notificação à CNPD da intenção de implementação da solução BYOD. • Processamento e transporte de dados sensíveis -obrigatório obter a autorização prévia da CNPD. • Dispositivos pessoais (dados pessoais) - tem cariz voluntário uma vez que a legislação portuguesa prevê que sejam as organizações a fornecerem os mecanismos necessários. O colaborador deve concordar por escrito com a política BYOD.	• Implementação de redes seguras: VPN. • Criptação dos discos. • Implementação de *container's* ("*sandboxs*") - separação dos dados corporativos dos dados pessoais. • Soluções MDM.	• Levantamento da legislação • Levantamento das possíveis sanções/coinas em caso de incumprimento	• Identificação das ameaças e vulnerabilidades que possam provocar possíveis quebras de segurança • Identificação dos riscos • Parecer das possíveis medidas de mitigação • Parecer sobre	• Apoio nas questões relacionadas com produtividade, pagamentos e custos laborais • Apoio no processo de consentimento dos colaboradores • Apoio no estabelecimento dos direitos, deveres e
	2. Possíveis quebras de segurança	• Informar clientes, autoridades, CNPD, de acordo com o tipo de dados envolvidos (sensíveis ou pessoais) e a gravidade da violação. • Exemplos: Lei 46/2012 de 20 de agosto	• Implementação de um politica BYOD com os termos e a condições admissíveis, assim como os direitos e deveres quer da organização quer dos colaboradores e as consequências por			

		(exemplo do número 10, do artigo 2º e número 1 e 2 do artigo 3º-A.	utilização incorreta. Envolvimento das áreas de tecnologia de informação (ICT), jurídico e recursos humanos (RH). • Divulgação e formação dos colaboradores.		a implementação de soluções ICT • Estabelecimento da política BYOD • Apoio no processo de elegibilidade (quem, ao quê, onde e quando) • Apoio nas questões de *awareness,* formação e controlo	consequências por utilização incorreta
	3. Regulação e legislação aplicável	• Recomendações sobre as melhores práticas relativas ao nível de segurança - O ICP - Autoridade Nacional de Comunicações (ICP - ANACOM). • Matérias de proteção de dados pessoais - Comissão Nacional de Proteção de Dados (CNPD). • Legislação portuguesa, por exemplo: Código do Trabalho, Lei 46/2012 de 20 de agosto, Lei 67/98, de 26 de outubro, etc.	• Avaliação dos requisitos da legislação considerando a legislação em vigor. • Revisão regular. • Divulgação e formação dos colaboradores. • Formação em termos de comportamentos perante ambientes menos seguros.			
	4. Requisitos legais aplicáveis aos territórios	• Legislação internacional • Legislação local				
Laborais	**5. Proteção dos dados pessoais**	• Consentimento por escrito da politica BYOD • Legislação portuguesa, por exemplo: número 1 do artigo 22º, do Código do Trabalho, número 1 do artigo 5º da Lei 46/2004 e o número 4 do artigo 6º da Lei 46/2004.	• Implementação da política BYOD com os termos e a condições admissíveis, assim como os direitos e deveres quer da organização quer dos colaboradores e as consequências por utilização incorreta. Envolvimento das áreas de recursos. • Divulgação da política e obtenção do consentimento dos colaboradores. • Formação dos colaboradores. • Implementação de soluções Cloud (SaaS) , Office365			
	6. Licenciamento de software e penalidades	• Legislação portuguesa, por exemplo: número 1 e 2 do artigo 6º da Lei 109/2009 de 15 de setembro				
	7. Riscos laborais	• Legislação portuguesa, por exemplo: Código do Trabalho, Lei 46/2004				

Anexo C – Identificação das medidas de mitigação e áreas de atuação

Áreas	Cenários de ameaças IT		Controlos de Segurança e/ou Medidas de Mitigação	
	Ameaças	**Risco**	**Descrição**	**Área de atuação**
1. Segurança Física	• Roubo ou perda de dispositivos móveis	• Comprometimento dos dados • Acesso não autorizado	• Autenticação forte	software
			• Autenticação multi-fator	software
			• Cifrar o dispositivo ou os dados sensíveis	software
			• Limpeza *(wipe)* remoto (Solução MDM)	software
			• Formação e *Awareness* (roubo e perda)	si
2. Dispositivos móveis	• *Malware*	• Acesso não autorizado • Integridade dos dados • Roubo de dados	• Tecnologias antimalware: software antivírus, *firewalls* e passwords	software
			• Soluções NAC (*Network Access Control*);	network
			• Redes separadas (rede própria para dispositivos externos, em vez de acederem diretamente à rede interna)	network
			• Aplicações de análise da integridade dos dispositivos	software
	• Sincronização entre dispositivos	• Fuga dos Dados	• Formação e *Awareness* (sincronização entre dispositivos)	si
		• Roubo de dados negócio e pessoais	• Restrição e ou proibição do uso de determinadas aplicações	si
		• Perda de propriedade intelectual	• Serviços de *Cloud Computing*	network
		• Imagem negativa		
		• Prejuízos financeiros		

	• Proliferação de dispositivos móveis	• Equipamentos obsoletos • Incapacidade de resposta IT para as alterações	• Restrição dos dispositivos móveis, versões e sistemas operativos com controlo efetivo	si
	• Utilização de software não licenciado	• Penalidades e coimas.	• Disponibilização de software e, ou serviços por assinatura (exemplo: SAAS, Office 365, etc.)	software
			• Formação e *Awareness* (licenciamento)	si
3. Rede	• Mecanismos de conectividade inseguros: *Bluetooth* e *Wi-Fi*	• Interceção e modificação das comunicações • Acesso não autorizado • Comprometimento de dados	• Criptografia forte (como redes privadas virtuais, VPNs)	network
			• Mecanismos de autenticação mútua (verificação da identidade em ambos os *endpoints*)	network
	• Ataques: Eavesdropping e Man-in-the-middle (MITM)		• Proibição do acesso a redes Wi-Fi inseguras, i.e., que executam protocolos com vulnerabilidades conhecidas	si
			• Desativação de interfaces de rede desnecessários	network
4. Aplicações	• Acesso externo a recursos internos	• Comprometimento dos recursos internos (Ex: servidores)	• Disponibilização do mínimo (acessos) necessário	si
			• Proibição da instalação de aplicações de terceiros	si
			• Criação de *whitelisting* das aplicações aprovadas	si
			• Implementação de *sandbox's/containers seguros* que isola os dados e as aplicações da organização de todos os outros dados e aplicações no dispositivo móvel	network
			• Realização de avaliação de risco para cada aplicação de terceiros antes de permitir a utilização nos dispositivos móveis da organização.	si

Anexo D – Tabela Impacto no negócio e Esforço de implementação

Valor	Valor relativo	Valores anuais	
		Impacto no Negócio	Esforço de Implementação
1	Muito baixo	Até 50.000€	Até 10.000€
2	Baixo	Entre 50.000 e 100.000€	Entre 10.000 e 30.000€
3	Médio	Entre 100.000 e 200.000€	Entre 30.000 e 50.000€
4	Alto	Entre 200.000 e 300.000€	Entre 50.000 e 70.000€
5	Muito Alto	Superior a 300.000€	Superior a 70.000€

Anexo E – Validações do modelo de posicionamento ICT

Instruções de Preenchimento:
Passo 1: *Marcar com "X" as colunas "A (Aplicável)" ou "N/A (Não aplicável)" para cada item identificado na coluna " Possíveis medidas de Mitigação".*
Passo 2: *Para cada item com "x" em "A (Aplicável)" preencher na "Situação Atual" se a medida de mitigação "E (Existe)" ou se requer Implementação "I (Implementar)".*
Passo 3: *Para cada item "I (implementar)", preencher na coluna "Impacto no Negócio" o valor (de 1 a 5) correspondente na tabela auxiliar de "Valores de Impacto no Negócio" considerando o valor anual expectável.*
Passo 4: *Novamente para cada item identificado na "Situação Atual" de "implementar", preencher na coluna "Esforço de Implementação" o valor (de 1 a 5) correspondente na tabela auxiliar de "Valores de Esforço de Implementação" considerando o valor CAPEX / OPEX anual expectável.*
NOTAS:
- *As colunas sombreadas na área destinada ao Modelo de posicionamento das ameaças versus medidas de mitigação ICT são relativas a fórmulas pelo que não devem ser alteradas, exceto se for identificado algum erro no código.*
- *Sempre que se verifique situações de incompatibilidade entre colunas, os erros são assinaladas numa cor diferente (exemplo: a vermelho).*

Áreas	Controlos de Segurança e/ou Medidas de Mitigação		Modelo de posicionamento das ameaças versus controlos de segurança e/ou medidas de mitigação ICT							
	Descrição	Área de atuação	1.Análise		2.Situação Atual		3.Impacto no Negócio		4.Esforço de Implementação	
			A	NA	Existe | Implementar	validação	Valor	validação	Valor	validação
1. Segurança Física	• Autenticação forte	software		x						
	• Autenticação multi-fator	software	x	x	implementar		5		4	
	• Cifrar o dispositivo ou os dados sensíveis	software	x		existe					
	• Limpeza *(wipe)* remoto (Solução MDM)	software	x		implementar		3		4	
	• Formação e *Awareness* (roubo e perda)	si	x		implementar		1		1	

2. Dispositivos móveis	• Tecnologias antimalware: software antivírus, *firewalls* e passwords	software	x		implementar		3		4	
	• Soluções NAC (*Network Access Control*);	network		x	implementar	**item diff Aplicável**				
	• Redes separadas (rede própria para dispositivos externos, em vez de acederem diretamente à rede interna)	network	x		implementar		5		3	
	• *Container's* ("*Sandboxs*") seguros nos dispositivos móveis	network	x		existe		5	**item diff Implementar**		
	• Aplicações de análise da integridade dos dispositivos	software		x						
	• Formação e *Awareness* (sincronização entre dispositivos)	si	x		implementar		1		1	
	• Restrição e ou proibição do uso de determinadas aplicações	si	x		existe					
	• Serviços de *Cloud Computing*	network	x		existe				3	**item diff implementar**
	• Restrição dos dispositivos móveis, versões e sistemas operativos com controlo efetivo	si	x		implementar		3		3	
	• Disponibilização de software e, ou serviços por assinatura (exemplo: SAAS, Office 365, etc.)	software	x		implementar		4		2	
	• Formação e *Awareness* (licenciamento)	si	x		implementar		1		1	
3. Rede	• Criptografia forte (como redes privadas virtuais, VPNs)	network	x	x	implementar		5		4	
	• Mecanismos de autenticação mútua (verificação da identidade em ambos os *endpoints*)	network	x		implementar		4		4	
	• Proibição do acesso a redes Wi-Fi inseguras, i.e., que executam protocolos com vulnerabilidades conhecidas	si	x		implementar		4		1	
	• Desativação de interfaces de rede desnecessários	network	x		implementar		4		1	

4. Aplicações	• Disponibilização do mínimo (acessos) necessário	si	x		existe					
	• Proibição da instalação de aplicações de terceiros	si	x		implementar		4		1	
	• Criação de *whitelisting* das aplicações aprovadas	si	x		implementar		4		1	
	• Implementação de *sandbox's/containers seguros* que isola os dados e as aplicações da organização de todos os outros dados e aplicações no dispositivo móvel	network		x						
	• Realização de avaliação de risco para cada aplicação de terceiros antes de permitir a utilização nos dispositivos móveis da organização.	si	x		existe					

A = Aplicável; NA = Não aplicável

Anexo F – Fatores CBA para implementação da solução BYOD

Áreas	Fatores	Aspetos a considerar	BYOD
1.Produtividade	Satisfação	Calcular a produtividade a partir de um dispositivo pessoal e a partir de um dispositivo corporativo; comparar os valores	Possível aumento de receitas, no entanto há que considerar possíveis distrações com assuntos pessoais (app sociais) ou com problemas de acesso aos aplicativos corporativos; Depende do grau de maturidade do colaborador e da solução BYOD.
	Flexibilidade	*anytime / anywhere*	
	Iniciativa	Disponibilidade adicional; novas tendências	
2.Dispositivos	Compra dos dispositivos	Custo atual do dispositivo; valor da sua amortização; (perda) descontos obtidos	Possível diminuição de custos, a não ser que seja considerado valores de comparticipação dos dispositivos ou programas do tipo *Corporate Owned, Personally Enabled* - COPE.
	Substituições dos dispositivos		Possível diminuição de custos, uma vez que para dispositivos pessoais os custos de substituição costumam ser da responsabilidade do colaborador.
3.Telecomunicações	Planos de voz e dados	Custo atual do plano; descontos obtidos; custo com processos de reembolso	Depende da existência de planos de voz e dados e dos valores considerados

4.Infraestrutura	Soluções MDM	Custos com sistemas *Mobile Device Management* - MDM, T*elecom Expense Management* - TEM ou E*nterprise Mobility Management* - EMM	Possível aumento de custos tendo em conta o custo de software (incluir custos de licenciamento, implementação e gestão).
	Soluções Cloud	Custos CAPEX e OPEX	Possível aumento dos custos; Depende da tecnologia já usada.
	Network		
5.Aplicações corporativas	Desenvolvimento de aplicações corporativas	Custo de desenvolvimento; custo de deployed; possibilidade de contratar o serviço a terceiros; vantagens relacionado com o acesso rápido à informação	Possível aumento dos custos; Depende do tipo de aplicações (legacy, web-oriented) e dos dispositivos autorizados.
	Licenciamento Software	Custos CAPEX e OPEX	Depende do atual número de licenças versus custo de um serviço do tipo SaaS (*Software as a Service.*
6.Suporte e Formação	Politica BYOD	Consolidação dos objetivos com o que é expectável	Aumento de custos (com a elaboração da politica e de programas de awareness específicos), mas que pode levar à redução de custos se for interiorizado pela organização (aumento do grau de maturidade em relação à solulção BYOD).
	Programas de *awareness*	Definição e criação de programas de *awareness* interna	
	Suporte *help-desk*	Custo com suporte a diferentes sistemas operativos (necessidade de equipas multidisciplinares)	Possível aumento de custos numa fase inicial, que pode ser diluído com um *help-desk* do tipo *self-service;* possibilidade de custos partilhados com a decisão em soluções MDM, que permitem gerir dispositivos remotamente (pelo próprio).

Anexo G – Questionário de Feedback

Avaliação do modelo de suporte à decisão para avaliação de soluções BYOD

Bom dia,

dedique, por favor, alguns minutos do seu tempo para preencher o questionário seguinte.

1

O modelo refere os aspectos mais importantes:

- Sim, refere
- Mais ou menos sim
- Normal
- Mais ou menos não
- Muito difícil

2

O modelo ajuda na decisão de avaliação da solução:

- Muito útil
- Mais ou menos útil
- Normal
- Mais ou menos inútil
- Absolutamente inútil

3

O interface apresentado é fácil de usar?

- Sim, muito
- Mais ou menos sim
- De dificuldade média
- Mais ou menos não
- Absolutamente não

4

A documentação que acompanha o modelo é:

- Muito útil
- Mais ou menos útil
- Normal
- Mais ou menos inútil
- Absolutamente inútil

5

O modelo ajuda na decisão de avaliação à solução BYOD:

- Muito útil
- Mais ou menos útil
- Normal
- Mais ou menos inútil
- Absolutamente inútil

6

Como avalia o funcionamento do modelo?

- Muito satisfeito/a
- Satisfeit/a
- Médio satisfeito/a
- Insatisfeito/a
- Muito insatisfeito/a

7

Recomendaria o modelo proposto?

- Definitivamente sim
- Provavelmente sim
- Não sei
- Provavelmente não
- Definitivamente não

8

Que outros elementos podem ser desenvolvidos?

Escreva um parágrafo

1500 caracteres restantes